

01000773003050012



ΕΦΗΜΕΡΙΣ ΤΗΣ ΚΥΒΕΡΝΗΣΕΩΣ

ΤΗΣ ΕΛΛΗΝΙΚΗΣ ΔΗΜΟΚΡΑΤΙΑΣ

ΤΕΥΧΟΣ ΠΡΩΤΟ **Αρ. Φύλλου 77**

30 Μαρτίου 2005

ΑΠΟΦΑΣΕΙΣ

Τροποποίηση της ΠΔ/ΤΕ 2438/1998, όπως ισχύει, σχετικά με το πλαίσιο αρχών λειτουργίας και κριτηρίων αξιολόγησης των Συστημάτων Εσωτερικού Ελέγχου των πιστωτικών ιδρυμάτων και με τον προσδιορισμό αρμοδιοτήτων των οργάνων τους στον τομέα του Εσωτερικού Ελέγχου.

ΤΡΑΠΕΖΑ ΤΗΣ ΕΛΛΑΔΟΣ
Η ΕΠΙΤΡΟΠΗ ΤΡΑΠΕΖΙΚΩΝ
ΚΑΙ ΠΙΣΤΩΤΙΚΩΝ ΘΕΜΑΤΩΝ

(Συνεδρίαση 193/11.3.2005, θέμα 1)

Αφού έλαβε υπόψη:

α) τις διατάξεις του άρθρου 18 του Ν. 2076/1992 «Ανάληψη και άσκηση δραστηριότητας πιστωτικών ιδρυμάτων και άλλες συναφείς διατάξεις», όπως ισχύει,

β) την ΠΔ/ΤΕ 2438/1998, όπως ισχύει, σχετικά με το πλαίσιο αρχών λειτουργίας και κριτηρίων αξιολόγησης των Συστημάτων Εσωτερικού Ελέγχου των πιστωτικών ιδρυμάτων και με τον προσδιορισμό αρμοδιοτήτων των οργάνων τους στον τομέα του Εσωτερικού Ελέγχου και ειδικότερα το κεφ. VI αυτής περί των βασικών αρχών και κριτηρίων λειτουργίας των συστημάτων πληροφορικής,

γ) την ΠΔ/ΤΕ 1313/9.6.88 «Στοιχεία που θα υποβάλλουν τα πιστωτικά ιδρύματα στην Τράπεζα της Ελλάδος για την άσκηση ελέγχου φερεγγυότητας, ρευστότητας και αποδοτικότητας», όπως ισχύει, και ειδικότερα την Κατάσταση 1 του Πίνακα Γ1 περί των προσώπων που έχουν ειδική σχέση με το πιστωτικό ίδρυμα,

δ) την από 21.2.2005 σχετική εισήγηση της Διεύθυνσης Εποπτείας Πιστωτικού Συστήματος της Τράπεζας της Ελλάδος,

ε) τη σκοπιμότητα περαιτέρω εξειδίκευσης του πιο πάνω πλαισίου, για την αποτελεσματικότερη και ασφαλέστερη λειτουργία των συστημάτων πληροφορικής, ως βασικής παραμέτρου της πρόληψης και αντιμετώπισης του λειτουργικού κινδύνου των πιστωτικών ιδρυμάτων, λαμβανομένων ιδίως υπόψη των εξελίξεων στον τομέα της ηλεκτρονικής τραπεζικής,

στ) την ανάγκη να διασφαλίζεται, μέσω κατάλληλων εσωτερικών εγκριτικών διαδικασιών κάθε πιστωτικού ιδρύματος, ότι οι όροι των πιστοδοτήσεων προς τα πρόσωπα που έχουν ειδική σχέση με αυτό δεν αποκλίνουν από την καταγεγραμμένη γενική πιστοδοτική του πολιτική, αποφάσισε τα ακόλουθα:

Συμπληρώνονται οι διατάξεις της ΠΔ/ΤΕ 2438/6.8.1998, ως εξής:

1. Η υποχρέωση λεπτομερούς καταγραφής των όρων και διαδικασιών λειτουργίας του πιστωτικού ιδρύματος, στο πλαίσιο εφαρμογής του κεφ. ΙΙΙ της ΠΔ/ΤΕ 2438/1998, αφορά και τις κάθε μορφής πιστοδοτήσεις ή συμμετοχές προς τα πρόσωπα που έχουν ειδική σχέση με το πιστωτικό ίδρυμα (σύμφωνα με τα οριζόμενα στην Κατάσταση 1 του Πίνακα Γ1 της ΠΔ/ΤΕ 1313/1988, όπως εκάστοτε ισχύει), ώστε να διασφαλίζεται ότι:

α) οι όροι των σχετικών πιστοδοτήσεων δεν αποκλίνουν από τους όρους που εφαρμόζονται στις αντίστοιχες κατηγορίες λοιπών χρηματοδοτήσεων, καθώς και

β) κάθε συμμετοχή ή πιστοδότηση στα πιο πάνω πρόσωπα πραγματοποιείται μετά από έγκριση του Διοικητικού Συμβουλίου ή απόφαση της Γενικής Συνέλευσης των μετόχων του πιστωτικού ιδρύματος, όπου κατά Νόμο απαιτείται.

Για τη διευκόλυνση της ομαλής χρηματοδοτικής κάλυψης των αναγκών της δραστηριότητας των επιχειρήσεων που συμπεριλαμβάνονται στα πρόσωπα που διατηρούν ειδική σχέση με το πιστωτικό ίδρυμα, κατά τα ανωτέρω, το Διοικητικό Συμβούλιο του πιστωτικού ιδρύματος μπορεί να καθορίζει ένα εύλογο όριο πιστοδοτήσεων μέχρι το οποίο δεν θα απαιτείται η προηγούμενη έγκριση του Δ.Σ., αλλά απλή γνωστοποίηση της αντίστοιχης πιστοδότησης.

2. Τα αναφερόμενα στην πιο πάνω παρ. 1 πρόσωπα που έχουν ειδική σχέση με το πιστωτικό ίδρυμα, οφείλουν να γνωστοποιούν στο Διοικητικό του Συμβούλιο το σύνολο του υφιστάμενου υπολοίπου των πιστοδοτήσεών τους από συνδεδεμένες με το πιστωτικό ίδρυμα επιχειρήσεις, κατά την έννοια του άρθρου 42ε του Ν. 2190/1920, όπως ισχύει, εντός 20 ημερών από το τέλος κάθε ημερολογιακού έτους. Η υποχρέωση αυτή είναι ανεξάρτητη από την υποβολή από το πιστωτικό ίδρυμα στην Τράπεζα της Ελλάδος υπολοίπων των σχετικών πιστοδοτήσεων, κατ' εφαρμογή της ΠΔ/ΤΕ 1313/1988, όπως εκάστοτε ισχύει.

3. α. Στο συνημμένο στην παρούσα απόφαση Παράρτημα, το οποίο αποτελεί εφεξής αναπόσπαστο τμήμα της ΠΔ/ΤΕ 2438/6.8.1998 (όπως συμπληρώνεται με την παρούσα απόφαση), καθορίζονται οι βασικές αρχές που οφείλουν να τηρούν για την ασφαλή και αποτελεσματική λειτουργία των συστημάτων πληροφορικής τα πιστωτικά

ιδρύματα, των οποίων το Σύνολο Ενεργητικού υπερβαίνει το ποσό των εκατό εκατομμυρίων (100.000.000) ευρώ.

β. Εξουσιοδοτείται η Διεύθυνση Εποπτείας Πιστωτικού Συστήματος της Τράπεζας της Ελλάδος να εξειδικεύει περαιτέρω τις διατάξεις της ΠΔ/ΤΕ 2438/6.8.1998, όπως συμπληρώνεται με την παρούσα απόφαση, καθώς και την έκταση συμμόρφωσης προς τις αρχές του πιο πάνω Παραρτήματος των πιστωτικών ιδρυμάτων, των οποίων το Σύνολο του Ενεργητικού υπολείπεται του ως άνω ελαχίστου ορίου.

Κατά τα λοιπά οι διατάξεις της ΠΔ/ΤΕ 2438/6.8.1998, όπως ισχύει, παραμένουν αμετάβλητες.

Από τις διατάξεις της παρούσας απόφασης δεν προκαλείται δαπάνη σε βάρος του Κρατικού Προϋπολογισμού.

Η απόφαση αυτή να δημοσιευθεί στην Εφημερίδα της Κυβερνήσεως.

Ο Πρόεδρος Τα Μέλη Ο Γραμματέας

Ακριβές αντίγραφο

Αθήνα, 21 Μαρτίου 2005

Ο Γραμματέας
Σ. ΠΑΠΑΔΟΠΟΥΛΟΣ

ΠΑΡΑΡΤΗΜΑ
(ΠΔ /ΤΕ 2438/1998)

ΑΡΧΕΣ ΑΣΦΑΛΟΥΣ ΚΑΙ ΑΠΟΤΕΛΕΣΜΑΤΙΚΗΣ ΛΕΙΤΟΥΡΓΙΑΣ ΤΩΝ ΣΥΣΤΗΜΑΤΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ ΣΤΑ ΠΛΑΙΣΙΑ ΤΗΣ ΔΙΑΧΕΙΡΙΣΗΣ ΤΟΥ ΛΕΙΤΟΥΡΓΙΚΟΥ ΚΙΝΔΥΝΟΥ ΑΠΟ ΤΑ ΠΙΣΤΩΤΙΚΑ ΙΔΡΥΜΑΤΑ

Περιεχόμενα

ΕΙΣΑΓΩΓΗ

Η Τράπεζα της Ελλάδος στο πλαίσιο των αρμοδιοτήτων της, προσδίδει ιδιαίτερη σημασία στην ασφαλή και αποτελεσματική λειτουργία των Συστημάτων Πληροφορικής των εποπτευομένων Πιστωτικών Ιδρυμάτων (ΠΙ). Το βασικό πλαίσιο αρχών και κριτηρίων για τα Πληροφοριακά Συστήματα (ΠΣ) τέθηκε με την Π.Δ./Τ.Ε. 2438/98 με στόχο την επάρκεια του συστήματος εσωτερικού ελέγχου. Η παρούσα θέτει ένα δομημένο και λεπτομερές πλαίσιο γενικών αρχών για την ασφαλή και αποτελεσματική λειτουργία των Πληροφοριακών Συστημάτων, λαμβάνοντας παράλληλα υπόψη τις πλέον πρόσφατες εξελίξεις της πληροφορικής στον βαθμό που επηρεάζουν την λειτουργία των ΠΙ. Το συγκεκριμένο πλαίσιο θα αποτελέσει τη βάση αξιολόγησης των Πιστωτικών Ιδρυμάτων στο συγκεκριμένο τομέα.

Η εφαρμογή του πλαισίου αρχών θα συμβάλλει σημαντικά στην αποτελεσματική διαχείριση του λειτουργικού κινδύνου που σχετίζεται με τα Πληροφοριακά Συστήματα. Η ανάγκη αυτή υπαγορεύεται και από το νέο σύστημα Κεφαλαιακής Επάρκειας των ΠΙ της Επιτροπής της Βασιλείας για την Τραπεζική Εποπτεία (Basel II), το οποίο εισάγει για πρώτη φορά τον λειτουργικό κίνδυνο στον υπολογισμό των κεφαλαιακών απαιτήσεων.

Οι αρχές αυτές ομαδοποιούνται σε τέσσερις ενότητες και συγκεκριμένα στις:

- Οργάνωση και Διοίκηση Πληροφορικής, όπου γίνεται αναφορά στην Διακυβέρνηση της Πληροφορικής, στην οργάνωση της Υπηρεσιακής Μονάδας της Πληροφορικής και στις σχέσεις με τους Εξωτερικούς Συνεργάτες.
- Ανάπτυξη και Προμήθεια Συστημάτων, όπου γίνεται αναφορά στις μεθοδολογίες, πρότυπα και διαδικασίες ανάπτυξης και προμήθειας Πληροφοριακών Συστημάτων
- Λειτουργία και Υποστήριξη, όπου γίνεται αναφορά στις διαδικασίες λειτουργίας των συστημάτων, στην φυσική και λογική τους ασφάλεια, καθώς και στην διασφάλιση της συνέχειας των εργασιών του ΠΙ.
- Έλεγχος Συστημάτων Πληροφορικής, όπου γίνεται αναφορά σε κανόνες και βασικές απαιτήσεις για την επαρκή και αποτελεσματική λειτουργία του Εσωτερικού Ελέγχου αναφορικά με τα Πληροφοριακά Συστήματα.

Α. ΟΡΓΑΝΩΣΗ ΚΑΙ ΔΙΟΙΚΗΣΗ ΠΛΗΡΟΦΟΡΙΚΗΣ

Α1. Διακυβέρνηση Πληροφορικής

Η Διακυβέρνηση της Πληροφορικής (Information Technology Governance) είναι ευθύνη της Διοίκησης του ΠΙ και αποτελεί αναπόσπαστο τμήμα της Εταιρικής Διακυβέρνησης (Corporate Governance). Περιλαμβάνει το σύνολο των κατάλληλων επιχειρησιακών δομών και διαδικασιών μέσω των οποίων διασφαλίζεται ότι η Πληροφορική υποστηρίζει τη στρατηγική και τους στόχους του ΠΙ, προσθέτει αξία στον οργανισμό, διαχειρίζεται αποτελεσματικά τους πόρους που της διατίθενται, αξιολογεί και διαχειρίζεται αποτελεσματικά τους κινδύνους που απορρέουν από την λειτουργία των Πληροφοριακών Συστημάτων, εφαρμόζει πιστά την Πολιτική Ασφάλειας, είναι σε θέση να μετρήσει την αποτελεσματικότητα και αποδοτικότητα της και τέλος υλοποιεί ένα σύνολο μηχανισμών ελέγχου στα πλαίσια ενός γενικότερου ελεγκτικού πλαισίου.

Για την επίτευξη των προαναφερθέντων το ΠΙ θα πρέπει:

1. να διαθέτει καταγεγραμμένη και εγκεκριμένη στρατηγική για την Πληροφορική, συμβατή με τη γενικότερη επιχειρησιακή στρατηγική του. Η στρατηγική της Πληροφορικής οφείλει, αφ' ενός μεν να υλοποιεί τους επιχειρησιακούς στόχους που έχουν τεθεί από τη Διοίκηση του ΠΙ, αφ' ετέρου δε να διαμορφώνει έγκαιρα την απαραίτητη τεχνολογική υποδομή για τις μελλοντικές ανάγκες του οργανισμού. Το ΠΙ πρέπει να διαθέτει τα κατάλληλα υπηρεσιακά όργανα και διαδικασίες για τη χάραξη της στρατηγικής της Πληροφορικής, την τήρηση και την περιοδική ενημέρωση της, ώστε να εναρμονίζεται διαρκώς με τους εκάστοτε επιχειρησιακούς στόχους και το εκάστοτε ισχύον θεσμικό πλαίσιο. Η εγκεκριμένη στρατηγική της Πληροφορικής πρέπει να περιλαμβάνει τόσο βραχυπρόθεσμα (ετήσια) όσο και μέσο - μακροπρόθεσμα (τριετή) σχέδια.

2. να διαθέτει ειδική συντονιστική επιτροπή για την Πληροφορική (I.T. Steering Committee). Επικεφαλής της επιτροπής συνιστάται να είναι μέλος της Διοίκησης με γνώση των θεμάτων πληροφορικής, και μέλη διευθυντικά στελέχη του οργανισμού. Ο ρόλος, τα καθήκοντα και η ελάχιστη σύνθεση της επιτροπής θα πρέπει να ορίζονται σε επίσημο κανονισμό. Στα καθήκοντα της επιτροπής, μεταξύ άλλων περιλαμβάνονται η αξιολόγηση των βραχυπρόθεσμων και μέσο - μακροπρόθεσμων σχεδίων της Πληροφορικής στα πλαίσια της επιχειρησιακής στρατηγικής, η αξιολόγηση της Ανάλυσης & Διαχείρισης των Κινδύνων που σχετίζονται με τα Πληροφοριακά Συστήματα, η αξιολόγηση και έγκριση μεγάλων προμηθειών υλικού και λογισμικού, η εποπτεία των μεγάλων έργων και του προϋπολογισμού της Πληροφορικής, ο καθορισμός προτεραιοτήτων, η αξιολόγηση πολιτικών, προτύπων και διαδικασιών, η έγκριση και εποπτεία των συνεργασιών με τρίτους (π.χ. θέματα outsourcing), κ.λπ. Η Επιτροπή, τέλος, θα πρέπει να λαμβάνει γνώση των πορισμάτων των ελέγχων που διενεργούνται στα Πληροφοριακά Συστήματα.

3. στο πλαίσιο της αρμόδιας υπηρεσιακής μονάδας Διαχείρισης Κινδύνων να αξιολογεί, κατηγοριοποιεί και διαχειρίζεται τους κινδύνους που απορρέουν από την ανάπτυξη, ενσωμάτωση και λειτουργία των Πληροφοριακών Συστημάτων. Οι κίνδυνοι αυτοί θα πρέπει να συνεκτιμούνται με τους υπόλοιπους κινδύνους στους οποίους είναι εκτεθειμένο το ΠΙ.

4. να διαθέτει καταγεγραμμένη και εγκεκριμένη από την Διοίκηση Πολιτική Ασφάλειας για τα Πληροφοριακά Συστήματα με τη μορφή αρχών - δεσμεύσεων, οι οποίες θα προδιαγράφουν τις κατευθύνσεις και τους στόχους του οργανισμού για την αποτελεσματική διαχείριση, προστασία και κατανομή των πληροφοριακών του πόρων. Η Πολιτική Ασφάλειας οφείλει,

(i) να παραπέμπει σε συγκεκριμένα πρότυπα και διαδικασίες δεσμεύοντας έτσι τις υπηρεσιακές μονάδες στην υλοποίηση και το προσωπικό στην τήρησή τους

(ii) να προσφέρει ένα κανονιστικό πλαίσιο βάσει του οποίου διενεργούνται οι έλεγχοι και

(iii) να προσαρμόζεται και ενημερώνεται βάσει θεσμοθετημένων διαδικασιών.

Το περιεχόμενο της Πολιτικής Ασφάλειας θα πρέπει να κοινοποιείται στο προσωπικό του ΠΙ και να υπάρχει από αυτό η έγγραφη αποδοχή του. Η ύπαρξη της Πολιτικής Ασφάλειας, οι στόχοι της, σύνοψή της, και το περιεχόμενο συγκεκριμένων τμημάτων της - αν αυτό απαιτείται -, μπορεί να γνωστοποιείται στο κοινό, έτσι ώστε να προάγεται το αίσθημα εμπιστοσύνης των πελατών απέναντι στο ΠΙ.

5. να διαθέτει, πέραν της Πολιτικής Ασφάλειας, την κατάλληλη διοικητική δομή που θα εγγυάται τη ασφάλεια των επιχειρησιακών πληροφοριών. Στο πλαίσιο αυτής της δομής θα πρέπει τουλάχιστον να προβλέπεται θέση Υπεύθυνου Ασφάλειας ΠΣ, η αμεροληψία και η ανεξαρτησία του οποίου θα πρέπει να διασφαλίζονται μέσω της απευθείας αναφοράς του σε υψηλά κλιμάκια της ιεραρχίας.

6. να μεριμνά ώστε οι υπάρχουσες πολιτικές, πρότυπα, διαδικασίες και μεθοδολογίες να είναι επίσημα καταγεγραμμένες και εγκεκριμένες από τα αρμόδια υπηρεσιακά όργανα.

7. να διαθέτει πρότυπα και μεθοδολογίες για το σχεδιασμό και την ανάπτυξη των Πληροφοριακών Συστημάτων, καθώς και διαδικασίες για την καθημερινή τους λειτουργία και υποστήριξη.

8. να διαθέτει πρότυπα και διαδικασίες για τη διαχείριση των έργων πληροφορικής. Στην πρόταση για την υλοποίηση κάθε μεγάλου έργου πληροφορικής πρέπει να προσδιορίζεται ο επιχειρησιακός στόχος, καθώς και τα ποιοτικά και ποσοτικά οφέλη που θα αποφέρει η υλοποίηση του. Η αποτελεσματική έκβαση ενός έργου διασφαλίζεται με την ύπαρξη και τήρηση καταλλήλων μεθοδολογιών και πρακτικών που ακολουθούνται σε όλο τον κύκλο ζωής του. Σε αυτές περιλαμβάνονται, η μεθοδολογία και τα εργαλεία παρακολούθησης του έργου, ο συντονισμός των απαιτούμενων ενεργειών και πόρων, η τήρηση χρονοδιαγραμμάτων, η παρακολούθηση του κόστους, η συμμετοχή των στελεχών τόσο της Πληροφορικής όσο και των άλλων επιχειρησιακών μονάδων στις διάφορες φάσεις υλοποίησης, η μεθοδολογία διαχείρισης αλλαγών, η εκπαίδευση του προσωπικού και Τέλος, η διασφάλιση της ποιότητας πρέπει να αποτελεί ανεξάρτητη διαδικασία στην οργάνωση και διαχείριση ενός έργου πληροφορικής.

9. να εγγυάται την ποιότητα των παρεχόμενων υπηρεσιών πληροφορικής μέσω της ύπαρξης διαδικασιών διασφάλισης ποιότητας και εναρμόνισης με τα πρότυπα ποιότητας που έχει θέσει το ΠΙ. Η ποιότητα πρέπει να διασφαλίζεται σε όλα τα στάδια του κύκλου ζωής των συστημάτων και να καλύπτει τα παραδοτέα, την τεκμηρίωση, την εκπαίδευση, τις προδιαγραφές, τις διαδικασίες, και τα σχέδια υλοποίησης ενός έργου.

10. να διαθέτει τις κατάλληλες διαδικασίες για τον έγκαιρο εντοπισμό και την αποτελεσματική αντιμετώπιση των προβλημάτων που προκύπτουν στα Πληροφοριακά Συστήματα.

11. να διαθέτει διαδικασίες καταγραφής και κατηγοριοποίησης των γεγονότων που δημιουργούν λειτουργικό κίνδυνο, συμπεριλαμβανομένων των ζημιών (detailed event type logging and classification) που προέρχονται από προβλήματα στα Πληροφοριακά Συστήματα (π.χ. μη εξουσιοδοτημένη δραστηριότητα, κλοπή μηχανογραφικού εξοπλισμού, απάτη, παραβίαση ασφάλειας, μη διαθεσιμότητα συστημάτων, καταστροφή μηχανογραφικού εξοπλισμού, κακόβουλη χρήση, κ.α. και ενημέρωσης των αρμόδιων υπηρεσιακών μονάδων (Διαχείρισης Κινδύνων και Εσωτερικού Ελέγχου), για την αποτελεσματικότερη καταγραφή και αντιμετώπιση του λειτουργικού κινδύνου. Η καταγραφή θα πρέπει να είναι συστηματική με στόχο την δημιουργία ιστορικότητας και λεπτομερής έτσι ώστε να περιγράφει με σαφήνεια το γεγονός. Οι σχετικές πληροφορίες θα πρέπει να καταγράφονται ηλεκτρονικά και να δομούνται με τέτοιο τρόπο ώστε να διευκολύνεται η αυτόματη παραγωγή αναφορών αλλά και η άμεση ενημέρωση των εμπλεκόμενων υπηρεσιακών μονάδων.

12. να διαθέτει Σύστημα Διοικητικής Πληροφόρησης (M.I.S. - Management Information System) κατάλληλο για την αποτελεσματική πληροφόρηση της Διοίκησης του οργανισμού. Ένα τέτοιο σύστημα θα πρέπει να χαρακτηρίζεται από την ομοιόμορφη και βάσει καταγεγραμμένων διαδικασιών συλλογή και επεξεργασία, την έγκαιρη διάθεση, την ακρίβεια, την αξιοπιστία, και την πληρότητα των πληροφοριών. Η συλλογή και επεξεργασία των απαραίτητων πληροφοριών θα πρέπει να γίνεται όσο το δυνατόν πιο αυτοματοποιημένα.

13. να γνωρίζει και να συμμορφώνεται με το νομικό, εποπτικό και κανονιστικό πλαίσιο σε ό,τι αφορά θέματα πληροφορικής.

14. να μελετά, να αξιολογεί και να εφαρμόζει, όπου κρίνει απαραίτητο, τα διεθνή πρότυπα και μεθοδολογίες διαχείρισης και ασφάλειας των Πληροφοριακών Συστημάτων, καθώς επίσης να παρακολουθεί και να λαμβάνει υπόψη τις διεθνείς εξελίξεις στους συγκεκριμένους τομείς.

Α2. Οργάνωση Υπηρεσιακής Μονάδας Πληροφορικής

Το Πιστωτικό Ίδρυμα θα πρέπει να διαθέτει εξειδικευμένη Υπηρεσιακή Μονάδα Πληροφορικής, λειτουργικά και διοικητικά ανεξάρτητη από τους τελικούς χρήστες των υπηρεσιών πληροφορικής η οποία θα πρέπει:

1. να διαθέτει οργανόγραμμα στο οποίο:

• απεικονίζονται οι επιχειρησιακές και οργανωτικές ανάγκες της μονάδας και περιγράφονται με σαφήνεια οι αρμοδιότητες των επί μέρους υπηρεσιακών μονάδων που το αποτελούν

• απεικονίζεται ο διαχωρισμός των καθηκόντων προκειμένου να αποκλείεται η ύπαρξη ασυμβίβαστων ρόλων, να παρέχεται η δυνατότητα καταλογισμού των ευθυνών και να αξιοποιούνται με τον καταλληλότερο τρόπο οι δυνατότητες του προσωπικού. Ειδικότερα, θα πρέπει να διασφαλίζεται ότι διαχωρίζονται πλήρως οι λειτουργίες που σχετίζονται με τον σχεδιασμό και την ανάπτυξη των συστημάτων από τις λειτουργίες που αφορούν στην καθημερινή λειτουργία τους

• προβλέπεται, ανάλογα με το μέγεθος του ΠΙ και την πολυπλοκότητα των συστημάτων, υπηρεσιακή μονάδα Ασφάλειας των ΠΣ. Η συγκεκριμένη υπηρεσιακή μονάδα, μαζί με τον Υπεύθυνο Ασφάλειας των ΠΣ, πρέπει να διαμορφώνουν ολοκληρωμένη εικόνα για το επίπεδο ασφάλειας των συστημάτων και τους κινδύνους που απορρέουν από την ανάπτυξη, ενσωμάτωση και λειτουργία τους. Στις αρμοδιότητες τους περιλαμβάνονται, μεταξύ άλλων, η συμμετοχή στην αξιολόγηση και διαχείριση των κινδύνων των ΠΣ, η σύνταξη και ενημέρωση της πολιτικής ασφάλειας, η συμμετοχή στη διαδικασία εύρεσης λύσεων για την κάλυψη κενών ασφάλειας και την αντιμετώπιση έκτακτων περιστατικών κ.α.

• εξασφαλίζεται η αναπλήρωση του προσωπικού τουλάχιστον στις κρίσιμες μηχανογραφικές λειτουργίες

2. να διαθέτει καταγεγραμμένες και επίσημα εγκεκριμένες περιγραφές θέσεων εργασίας στις οποίες θα περιλαμβάνονται οι αρμοδιότητες, οι υπευθυνότητες και οι δεξιότητες που απαιτούνται για κάθε θέση.

Α3. Σχέσεις με Εξωτερικούς Συνεργάτες

Όταν το ΠΙ συνεργάζεται με εξωτερικούς συνεργάτες σε θέματα πληροφορικής (Πάροχοι Υπηρεσιών Πληροφορικής - Π.Υ.Π., προμηθευτές, κ.λπ.), θα πρέπει να λαμβάνει υπόψη του ότι:

1. η χρήση εξωτερικών συνεργατών, ενώ μπορεί να επιλύει σημαντικά προβλήματα, δημιουργεί πεδίο πρόσθετων κινδύνων για το ΠΙ, οι οποίοι πρέπει να εντοπισθούν, εκτιμηθούν και αντιμετωπισθούν αποτελεσματικά. Στους κινδύνους αυτούς περιλαμβάνονται:

• η έλλειψη ουσιαστικού ελέγχου στις προσφερόμενες υπηρεσίες

• η εξάρτηση από τρίτους

• η απώλεια εσωτερικής τεχνογνωσίας

• η ενδεχόμενη αδυναμία άμεσης προσαρμογής στις απαιτήσεις των πελατών και του οικονομικού περιβάλλοντος

• η αδιαφανής κοστολόγηση των προσφερόμενων υπηρεσιών

• η αντίδραση του προσωπικού που θίγεται από την χρήση υπηρεσιών εξωτερικών συνεργατών

• η διαφορά νοοτροπίας μεταξύ ΠΙ και παρόχου, κ.λπ.

2. σε περίπτωση που αποφασίσει να αναθέσει μέρος ή και το σύνολο των υπηρεσιών πληροφορικής σε εξωτερικούς συνεργάτες, πρέπει να υφίστανται κατάλληλες διαδικασίες για:

• την αξιολόγηση των κινδύνων που απορρέουν από μια πιθανή συνεργασία

• τον τρόπο επιλογής των εξωτερικών συνεργατών

• την επάρκεια των προς υπογραφή συμβολαίων

• την εποπτεία και τον έλεγχο της επαρκούς και ασφαλούς λειτουργίας των συστημάτων

3. η ανάθεση υλοποίησης σημαντικών για το ΠΙ συστημάτων σε τρίτους, θα πρέπει να αιτιολογείται από την Ειδική Συντονιστική Επιτροπή Πληροφορικής εγγράφως προς τη Διοίκηση ο οποία και παρέχει την τελική έγκριση της.

4. κατά το στάδιο της επιλογής του εξωτερικού συνεργάτη, πέραν της αξιολόγησης των Προσφερομένων υπηρεσιών θα πρέπει να αξιολογούνται, με βάση το μέγεθος και την κρισιμότητα της συνεργασίας:

• η οικονομική κατάσταση και η μακροπρόθεσμη βιωσιμότητα του

• η επίδραση του προς υπογραφή συμβολαίου στον κύκλο εργασιών του

• η φήμη του στην αγορά, το πελατολόγιο και ο βαθμός ικανοποίησης των πελατών του

• η οργανωτική του δομή (για την παροχή και αποτελεσματική υποστήριξη των υπηρεσιών)

• η αριθμητική και ποιοτική επάρκεια του στελεχικού δυναμικού

• η ασφαλιστική του κάλυψη, κ.λπ.

Στις περιπτώσεις που ο εξωτερικός συνεργάτης κάνει χρήση συνεργιών για την υλοποίηση των έργων θα πρέπει να αξιολογηθούν ανάλογα και οι συνέργιες αυτές.

5. από τεχνικής άποψης θα πρέπει να αξιολογούνται:

• η ποιότητα και επάρκεια της υπάρχουσας Πολιτικής Ασφάλειας του παρόχου

• η αξιοπιστία των συστημάτων

• η καταλληλότητα της τεχνολογίας που χρησιμοποιείται

• η πληρότητα των διαδικασιών υποστήριξης των παρεχομένων υπηρεσιών

• τα σχέδια συνέχειας εργασιών και ανάκαμψης από καταστροφή του παρόχου

Πορίσματα εσωτερικών και εξωτερικών ελεγκτών για τον εξωτερικό συνεργάτη - εάν είναι διαθέσιμα - αποτελούν πολύτιμες πηγές πληροφόρησης για τη διαμόρφωση πληρέστερης εικόνας.

6. στο προς υπογραφή συμβόλαιο θα πρέπει - μεταξύ άλλων - να περιγράφονται αναλυτικά και με σαφήνεια:

• τα δικαιώματα και οι υποχρεώσεις των συμβαλλομένων μερών

• το συμφωνηθέν επίπεδο παροχής υπηρεσιών (Service Level Agreement - SLA) και ο τρόπος τιμολόγησης τους

• η δυνατότητα επαναδιαπραγμάτευσης του συμβολαίου

• τα θέματα ιδιοκτησίας (ownership), αδειοδότησης (licensing) και πνευματικών δικαιωμάτων

• οι περιπτώσεις υπεργολαβίας (sub-contracting)

• οι διαδικασίες επίλυσης διαφορών

• οι διαδικασίες τερματισμού του συμβολαίου (π.χ. οι διαδικασίες παράδοσης του πηγαίου κώδικα και των δεδομένων τους - Escrow Agreement)

Ειδική αναφορά θα πρέπει επίσης να γίνεται:

- στην ασφάλεια (εμπιστευτικότητα, ακεραιότητα, διαθεσιμότητα και δυνατότητα ανίχνευσης) των πληροφοριών
- στην πιστοποίηση των συναλλασσομένων μερών και στη μη αποποίηση των συναλλαγών
- στην ασφάλεια των διασυνδέσεων μεταξύ του ΠΙ και του εξωτερικού συνεργάτη
- στις ποινικές ρήτρες για τις περιπτώσεις παραβίασης των συμφωνηθέντων
- στη δυνατότητα διενέργειας ελέγχων εκ μέρους του ΠΙ (Right to Audit)
- στη δυνατότητα διενέργειας ελέγχων από τρίτους για λογαριασμό του ΠΙ
- στο είδος και τη συχνότητα των αναφορών ή αρχείων που θα ανταλλάσσουν τα δύο μέρη
- στα σχέδια συνέχειας εργασιών και ανάκαμψης από καταστροφή του εξωτερικού συνεργάτη

Β. ΑΝΑΠΤΥΞΗ ΚΑΙ ΠΡΟΜΗΘΕΙΑ ΣΥΣΤΗΜΑΤΩΝ

Ο κύκλος ζωής ενός συστήματος πρέπει να χαρακτηρίζεται από διακριτές φάσεις οι οποίες θα υλοποιούν πρότυπα, μεθοδολογίες και διαδικασίες επίσημα καταγεγραμμένες και εγκεκριμένες. Τέτοιες φάσεις, συνήθως, είναι η φάση της Μελέτης Σκοπιμότητας, της Ανάλυσης των Επιχειρησιακών Απαιτήσεων και του Καθορισμού των Προδιαγραφών, της Τεχνικής Ανάλυσης και του Σχεδιασμού, της Ανάπτυξης, των Δοκιμών, της Αποδοχής και της Μεταφοράς στην Παραγωγή, της Λειτουργίας και Υποστήριξης και τέλος της Απόσυρσης. Η μετάβαση από τη μία φάση στην άλλη προϋποθέτει την ανασκόπηση και έγκριση των αποτελεσμάτων της προηγούμενης.

Η εποπτεία του έργου της ανάπτυξης κάθε σημαντικού συστήματος πρέπει να ανατίθεται στη συντονιστική επιτροπή της Πληροφορικής (IT Steering Committee). Με την ολοκλήρωση της ανάπτυξης του συστήματος, η επιχειρησιακή και τεχνική του εποπτεία θα πρέπει να ανατίθεται στις αρμόδιες υπηρεσιακές μονάδες ή στελέχη.

Πριν την ανάπτυξη ή προμήθεια ενός σημαντικού συστήματος πρέπει να γίνεται Μελέτη Σκοπιμότητας. Στη φάση αυτή θα πρέπει μεταξύ άλλων να ορίζονται οι λειτουργίες που θα καλύπτονται από το νέο σύστημα, να εκτιμάται η σχέση κόστους / οφέλους (μείωση στα τρέχοντα κόστη, αύξηση απόδοσης, βελτίωση της εικόνας του ΠΙ) που θα επιφέρει το νέο σύστημα, και να εξετάζεται η δυνατότητα υλοποίησης του συστήματος τόσο από την πλευρά του ανθρώπινου δυναμικού όσο και από αυτή του μηχανογραφικού εξοπλισμού / λογισμικού. Τέλος, θα πρέπει να εκτιμάται το κόστος ανάπτυξης, λειτουργίας, και υποστήριξης του συστήματος και να συγκρίνεται το κόστος εσωτερικής ανάπτυξης με αυτό της προμήθειας ή της ανάθεσης σε τρίτους.

Β1. Ανάπτυξη Συστημάτων

Στις περιπτώσεις που το ΠΙ επιλέγει την εσωτερική ανάπτυξη ενός Πληροφοριακού Συστήματος, θα πρέπει:

1. πριν την έναρξη της ανάπτυξης, να ορισθεί Ομάδα Έργου που θα αναλάβει την διαχείριση του έργου και την κατάρτιση ενός χρονοδιαγράμματος υλοποίησης. Η Ομάδα Έργου ανάλογα με την κρισιμότητα και το μέγεθος του συστήματος θα πρέπει να απαρτίζεται από τον επικεφαλή της, τον υπεύθυνο για την ασφάλεια του συστήματος, αναλυτές / προγραμματιστές και εκπροσώπους χρηστών ή άλλων εμπλεκόμενων μερών.

2. το χρονοδιάγραμμα υλοποίησης να προσδιορίζει, μεταξύ άλλων, τις φάσεις, τη διάρκεια τους, και τους υπεύθυνους για την υλοποίηση της κάθε φάσης καθώς και τα παραδοτέα. Επιπλέον στο χρονοδιάγραμμα θα πρέπει να προβλέπεται ο ακριβής χρόνος παράδοσης μηχανογραφικού εξοπλισμού και άλλων υπηρεσιών από προμηθευτές εφόσον επηρεάζει τον χρονοπρογραμματισμό του έργου.

3. να ορίζεται ένα σχέδιο επικοινωνίας στο οποίο θα καθορίζονται οι διαδικασίες ενημέρωσης των εμπλεκομένων μερών για την πρόοδο του έργου, επικοινωνίας των θεμάτων προς επίλυση προς τα ανώτερα στελέχη, επικοινωνίας του Πιστωτικού Ιδρύματος με προμηθευτές, και κοινοποίησης των αλλαγών που θα επιφέρει το νέο σύστημα στον οργανισμό.

4. να λαμβάνονται υπόψη θέματα αποδοχής και αποτελεσματικής λειτουργίας του νέου πληροφοριακού συστήματος από το προσωπικό του Πιστωτικού Ιδρύματος και να υιοθετείται σχέδιο διαχείρισης των λειτουργικών αλλαγών ώστε να αντιμετωπιστούν φαινόμενα αρνητικής στάσης των χρηστών και μη αποτελεσματικής εξυπηρέτησης των πελατών λόγω έλλειψης εξοικείωσης με το νέο πληροφοριακό σύστημα.

5. οι πληροφορίες που συλλέγονται κατά την διάρκεια της φάσης της Ανάλυσης των Επιχειρησιακών Απαιτήσεων και του Καθορισμού των Προδιαγραφών, να αφορούν τα προβλήματα, τις απαιτήσεις και τις ανάγκες βελτίωσης που έχουν εντοπίσει οι χρήστες σχετικά με το σύστημα. Οι απαιτήσεις θα πρέπει να καθορίζουν το τι πρέπει να κάνει το σύστημα και όχι το πώς, ενώ οι προδιαγραφές θα πρέπει να προσδιορίζουν σε γενικές γραμμές το πώς θα μπορέσουν να υλοποιηθούν οι απαιτήσεις των χρηστών. Κατά τη φάση του καθορισμού των προδιαγραφών του νέου συστήματος θα πρέπει να εξεταστεί κατά πόσο αυτό θα πρέπει να συνεργάζεται και σε ποιο επίπεδο με τα υπάρχοντα συστήματα του ΠΙ

6. να γίνεται εκτίμηση του όγκου των δεδομένων και του αριθμού των συναλλαγών που θα διαχειρίζεται το νέο σύστημα, λαμβάνοντας υπόψη τις τρέχουσες αλλά και τις μελλοντικές ανάγκες έτσι ώστε να προσδιοριστούν με μεγαλύτερη ακρίβεια οι προδιαγραφές του μηχανογραφικού εξοπλισμού του συστήματος.

7. να γίνει λεπτομερής σχεδιασμός για την διαχείριση των δεδομένων του προϋπάρχοντος μηχανογραφικού ή μη συστήματος και να περιλαμβάνει θέματα εκκαθάρισης παλαιών δεδομένων (data cleansing), μετατροπής δεδομένων στην μορφή του νέου συστήματος (data conversion) και μετάπτωσης δεδομένων (data migration).

8. στις φάσεις της Τεχνικής Ανάλυσης και του Σχεδιασμού να διενεργείται Ανάλυση Κινδύνων και να καθορίζονται με λεπτομέρεια οι απαιτήσεις ασφαλούς λειτουργίας του συστήματος σύμφωνα και με όσα προβλέπει η ισχύουσα Πολιτική Ασφάλειας του ΠΙ, οι τεχνικές προδιαγραφές του (οι οποίες περιλαμβάνουν - μεταξύ άλλων - τον καθορισμό των παραμέτρων της λογικής ασφάλειας του συστήματος), ο έλεγχος και η συμφωνία των δεδομένων και η δομή των απαραίτητων αρχείων καταγραφής (audit trails και logs) για τα οποία θα πρέπει να λαμβάνονται υπόψη οι σχετικές συστάσεις της Ευρωπαϊκής Επιτροπής για τα Τραπεζικά Πρότυπα («The Use of Audit Trails in Security Systems: Guidelines for European Banks»).

Στις συγκεκριμένες φάσεις είναι αναγκαία η συνεργασία με τον Εσωτερικό Έλεγχο για τη διαμόρφωση των κατάλληλων δικλείδων ασφαλείας, καθώς και των ελεγκτικών αρχείων καταγραφής και αναφορών που θα παράγο-

νται για τη διευκόλυνση του ελέγχου. Η συνεργασία αυτή δεν επηρεάζει το ελεγκτικό έργο του Εσωτερικού Ελέγχου για το εν λόγω σύστημα.

9. η Ανάπτυξη του Συστήματος να υλοποιείται σε ξεχωριστό μηχανογραφικό περιβάλλον από αυτό της παραγωγής και να ακολουθεί πρότυπα που έχουν τεθεί από το ΠΙ (π.χ. χρήση συγκεκριμένων εργαλείων και μεθοδολογίας ανάπτυξης προγραμμάτων) με στόχο την ομοιογένεια των Πληροφοριακών Συστημάτων και την ευκολία υποστήριξης τους.

10. οι Δοκιμές του Συστήματος να διενεργούνται σε πρώτη φάση από το προσωπικό της Πληροφορικής σε ξεχωριστό περιβάλλον με προκαθορισμένα σενάρια. Σε δεύτερη φάση θα πρέπει να γίνονται τεκμηριωμένες και ολοκληρωμένες δοκιμές που περιλαμβάνουν:

• δοκιμές επαναφοράς (recovery testing) ελέγχοντας την δυνατότητα επαναφοράς του συστήματος σε περιπτώσεις βλάβης του λογισμικού ή του μηχανογραφικού εξοπλισμού

• δοκιμές ασφαλείας (security testing) ελέγχοντας ότι το σύστημα περιλαμβάνει τις δικλείδες ασφαλείας όπως αυτές προδιαγράφηκαν κατά τον σχεδιασμό του συστήματος

• δοκιμή αντοχής (stress test) του συστήματος σε συνθήκες επεξεργασίας αυξημένου όγκου δεδομένων

Στις δοκιμές αυτές είναι απαραίτητο να συμμετέχουν, πέραν των προγραμματιστών, η μονάδα Διασφάλισης Ποιότητας (όπου υπάρχει), ο Υπεύθυνος Ασφάλειας (Security Officer) και η μονάδα του Εσωτερικού Ελέγχου.

11. για την Αποδοχή του Συστήματος να διενεργούνται ολοκληρωμένες δοκιμές με όσο το δυνατόν πιο πιστή προσομοίωση των συνθηκών παραγωγής. Στην περίπτωση που νέο σύστημα αντικαθιστά παλαιότερο, θα πρέπει τα δύο συστήματα για ένα χρονικό διάστημα να λειτουργήσουν παράλληλα με τα ίδια δεδομένα (parallel run) και να γίνεται σύγκριση των αποτελεσμάτων τους. Οι συμμετέχοντες θα πρέπει να αποφασίζουν για την αποδοχή ή μη του συστήματος και γνωστοποιούν εγγράφως την απόφαση τους.

12. η Μεταφορά του νέου Συστήματος στην παραγωγή να πραγματοποιείται από εξειδικευμένο προσωπικό (π.χ. librarians) βάσει καταγεγραμμένων οδηγιών, σε χρονική περίοδο που δεν εκτελούνται άλλες σημαντικές εργασίες, και με τη πρόβλεψη για τη δυνατότητα - σε περίπτωση προβλήματος - επαναφοράς στην αρχική κατάσταση.

13. το σύστημα, πριν ακόμη τεθεί σε λειτουργία, να διαθέτει πλήρη τεκμηρίωση που θα ακολουθεί συγκεκριμένα ποιοτικά πρότυπα που έχουν τεθεί από το ίδιο το ΠΙ Τα εγχειρίδια της τεκμηρίωσης θα πρέπει να έχουν ενιαία μορφή και δομή.

14. να πραγματοποιείται εκπαίδευση των χρηστών του συστήματος σε ξεχωριστό μηχανογραφικό περιβάλλον το οποίο και δεν θα επηρεάζεται από τα μηχανογραφικά περιβάλλοντα ανάπτυξης και παραγωγής. Τα συγκεκριμένα περιβάλλοντα συνιστάται να παραμένουν ενεργά έτσι ώστε να χρησιμοποιούνται στις περιπτώσεις που το σύστημα υφίσταται αλλαγές.

15. η Λειτουργία και Υποστήριξη του Συστήματος να περιλαμβάνει διαδικασίες ελέγχου των αλλαγών (change control), ελέγχου των εκδόσεων του συστήματος (versioning), ελέγχου ενημερώσεων του συστήματος για την αντιμετώπιση προβλημάτων που εντοπίστηκαν (patching), ελέγχου της απόδοσης του συστήματος, λήψης και φύλαξης εφεδρικών αρχείων, συνέχειας των εργασιών, ενημέρωσης του Help Desk για την υποστήριξη των χρηστών του συστήματος, κ.α.

16. η φάση Απόσυρσης του Συστήματος να περιλαμβάνει διαδικασίες για τη διατήρηση των πληροφοριών σύμφωνα με τις νομικές και εποπτικές οδηγίες (information preservation), τη διαγραφή των πληροφοριών από τα μέσα αποθήκευσης (media sanitization), την απόσυρση του υλικού και λογισμικού (hardware & software disposal). Στη συγκεκριμένη φάση πρέπει να διασφαλίζεται η αποτελεσματική συνέχεια της λειτουργίας των συστημάτων που διασυνδέονται με το σύστημα που αποσύρεται.

Β2. Προμήθεια Συστημάτων

Στις περιπτώσεις που το ΠΙ αποφασίζει την προμήθεια Πληροφοριακών Συστημάτων, θα πρέπει, εκτός των προαναφερθέντων:

1. η όλη διαδικασία προμήθειας να χαρακτηρίζεται από διακριτές φάσεις οι οποίες θα υλοποιούν πρότυπα, μεθοδολογίες και διαδικασίες επίσημα καταγεγραμμένες και εγκεκριμένες. Τέτοιες φάσεις, είναι αυτές της πρόσκλησης για υποβολή προτάσεων (Request For Proposal - RFP) με αναλυτική περιγραφή των αναγκών που θα καλύπτει το προς προμήθεια σύστημα, της επιλογής του εξωτερικού συνεργάτη, της σύναψης της συμφωνίας και της υπογραφής του συμβολαίου, της ένταξης και λειτουργίας των συστημάτων στην παραγωγή, και τέλος της εποπτείας και του ελέγχου τους.

2. η επιλογή του συστήματος να γίνεται με βάση τις αναλυτικές προδιαγραφές που οφείλει να θέτει το ΠΙ, τις δυνατότητες επέκτασης και προσαρμογής του στις διαρκώς αυξανόμενες επιχειρησιακές ανάγκες, τη φιλικότητα προς τον χρήστη, τις δυνατότητες ασφαλούς λειτουργίας (λογική ασφάλεια, audit trails & logs), το επίπεδο υποστήριξης, το σύστημα αναφορών του, κ.α.

3. το είδος παρέμβασης του ΠΙ στο σύστημα να είναι εκ των προτέρων αυστηρά καθορισμένο. Οι όποιες παρεμβάσεις θα πρέπει να ακολουθούν εγκεκριμένες και καταγεγραμμένες διαδικασίες, να υλοποιούνται από εξειδικευμένο προσωπικό και να διατηρούνται στο ελάχιστο δυνατό επίπεδο έτσι ώστε να μην αλλοιώνεται η φυσιογνωμία του συστήματος και να είναι εύκολη η αναβάθμιση και συντήρηση του. Ας σημειωθεί ότι, σε περίπτωση σημαντικής απόκλισης των λειτουργικών διαδικασιών του ΠΙ από εκείνες που υποστηρίζει το αγορασθέν σύστημα, το ΠΙ είναι αυτό που συνήθως θα πρέπει να προσαρμόσει τις λειτουργικές του διαδικασίες στα χαρακτηριστικά του συστήματος και όχι το αντίστροφο.

4. στα κεντρικά συστήματα τραπεζικών εργασιών, η ανάγκη για ανάπτυξη περιφερειακών εφαρμογών που θα αντλούν πληροφορίες από το κεντρικό σύστημα και θα υλοποιούν τοπικές αλλά και επιχειρησιακές ιδιαιτερότητες να γίνεται με βάση τα ισχύοντα στο ΠΙ πρότυπα για την ανάπτυξη εφαρμογών, έτσι ώστε να διατηρείται η μηχανογραφική ομοιογένεια.

5. ο τρόπος υποστήριξης των συστημάτων να είναι αυστηρά προδιαγεγραμμένος, με σαφή καθορισμό των περιπτώσεων στις οποίες απαιτείται υποστήριξη από τον πάροχο αλλά και των χρονικών περιθωρίων ανταπόκρισης του.

6. οι περιπτώσεις απομεμακρυσμένης πρόσβασης του παρόχου στα συστήματα του ΠΙ για την επίλυση εκτάκτων προβλημάτων, να είναι εξαιρετικά περιορισμένες, να αντιμετωπίζονται με ιδιαίτερη προσοχή, και σε κάθε περίπτωση να υπάρχει πλήρης καταγραφή (logging) των ενεργειών του.

7. να είναι απαραίτητη η απόκτηση τεχνογνωσίας, όχι μόνον μέσω της κατάλληλης εκπαίδευσης του εμπλεκόμενου στη λειτουργία τέτοιων συστημάτων προσωπικού, αλλά κυρίως μέσω της συμμετοχής του σε όλες τις φάσεις εξέλιξης των συστημάτων, έτσι ώστε η εξάρτηση του ΠΙ από τον προμηθευτή βαθμιαία να ελαττώνεται.

8. εφόσον έχουν υλοποιηθεί οι απαιτήσεις του Πιστωτικού Ιδρύματος - όπως αυτές αναφέρονται στο συμβόλαιο - και μετά το πέρας των απαραίτητων δοκιμών εκ μέρους του παρόχου, να υφίσταται διαδικασία επίσημης αποδοχής και παραλαβής του συστήματος εκ μέρους του ΠΙ με την συμμετοχή όλων των εμπλεκομένων μερών.

Γ. ΛΕΙΤΟΥΡΓΙΑ ΚΑΙ ΥΠΟΣΤΗΡΙΞΗ

Η απρόσκοπτη λειτουργία των Πληροφοριακών Συστημάτων και η αποτελεσματική υποστήριξη τους είναι παράγοντες κρίσιμοι τόσο για την εύρυθμη λειτουργία του ΠΙ και τη δημιουργία σχέσεων εμπιστοσύνης με τους πελάτες, όσο και για την αποτελεσματική αντιμετώπιση του λειτουργικού κινδύνου. Η απρόσκοπτη λειτουργία και η αποτελεσματική υποστήριξη των Πληροφοριακών Συστημάτων προϋποθέτουν την τήρηση των πολιτικών, προτύπων και διαδικασιών του ΠΙ από όλες τις εμπλεκόμενες υπηρεσιακές μονάδες, αλλά και τους παρόχους υπηρεσιών πληροφορικής.

Γ1. Λειτουργία Συστημάτων

Ο όρος «Λειτουργία Συστημάτων» αναφέρεται στο σύνολο των διαδικασιών που απαιτούνται για την καθημερινή λειτουργία των Πληροφοριακών Συστημάτων σε ένα Πιστωτικό Ίδρυμα. Για ένα αποδεκτό επίπεδο ασφαλούς και αποτελεσματικής λειτουργίας τους θα πρέπει να υφίστανται:

1. πλήρης και λεπτομερής καταγραφή του μηχανογραφικού εξοπλισμού (κεντρικά συστήματα, εξυπηρετητές, προσωπικοί υπολογιστές, περιφερειακά, δίκτυα και τηλεπικοινωνίες), του αρχιτεκτονικού σχεδιασμού, του χρησιμοποιούμενου λογισμικού, καθώς και του ιστορικού των εκδόσεων, των ενημερώσεων, και των αδειών χρήσης. Αρχείο πρέπει να τηρείται επίσης για τα μέσα που αποθηκεύουν και διακινούν ευαίσθητα δεδομένα του οργανισμού (cartridges, ταινίες, δισκέτες, CDs, εκτυπώσεις, microfiche κα). Τα αρχεία καταγραφής θα πρέπει να ενημερώνονται άμεσα στις περιπτώσεις αλλαγών.

2. τήρηση πλήρους και ενημερωμένης τεκμηρίωσης για κάθε σύστημα με τα επίσημα εγχειρίδια των εταιρειών που προμηθεύουν το υλικό και το λογισμικό των συστημάτων, και τα εγχειρίδια που συντάσσονται από το προσωπικό του ΠΙ.

3. επαρκής συντήρηση και τεχνική υποστήριξη των συστημάτων με βάση πάντοτε τις προδιαγραφές τους και τις ανάγκες που προκύπτουν.

4. υποστήριξη των υπαλλήλων-χρηστών εντός, αλλά και των πελατών - χρηστών εκτός του οργανισμού (π.χ. ηλεκτρονική τραπεζική), η οποία και θα πρέπει να ανατίθεται σε κατάλληλα οργανωμένες και στελεχωμένες υπηρεσιακές μονάδες (Help Desk). Στην υποστήριξη θα πρέπει να λαμβάνεται υπόψη το είδος του χρήστη και η φύση του προβλήματος που αντιμετωπίζει. Το πλήθος και το είδος των προβλημάτων θα πρέπει να καταγράφονται και να τυγχάνουν στατιστικής επεξεργασίας.

5. διαδικασίες διαχείρισης των παραμέτρων λειτουργίας των συστημάτων.

6. διαδικασίες αποτροπής εγκατάστασης και χρήσης μη νόμιμου, χωρίς την κατάλληλη αδειοδότηση, λογισμικού.

7. προγραμματισμός των εργασιών προς εκτέλεση, καταγραφή των προβλημάτων που προκύπτουν και των ενεργειών που πρέπει να γίνονται στις έκτακτες περιπτώσεις, κ.λπ. Η επιτυχής ή μη εκτέλεση των προγραμματισμένων αλλά και έκτακτων εργασιών θα πρέπει να καταχωρείται σε ειδικό ημερολόγιο, το οποίο και θα φέρει τις υπογραφές του προσωπικού που τις εκτέλεσε. Η εκτέλεση έκτακτων εργασιών θα πρέπει να γίνεται κατόπιν ειδικής έγκρισης.

8. έλεγχος των δεδομένων, για εξασφάλιση της ακεραιότητας, ορθότητας και εμπιστευτικότητας τους, σε όλες τις φάσεις επεξεργασίας τους. Οι κάθε είδους ασυμφωνίες θα πρέπει να διαπιστώνονται και να αντιμετωπίζονται βάσει καταγεγραμμένων διαδικασιών.

9. διαδικασίες διαχείρισης της χωρητικότητας, του φόρτου και της απόδοσης των συστημάτων και δικτύων.

10. συνεχής παρακολούθηση της διαθεσιμότητας των συστημάτων και των δικτύων. Ειδικότερα για τα κρίσιμα συστήματα, το ΠΙ πρέπει να είναι σε θέση να υπολογίζει το ποσοστό διαθεσιμότητας τους σε επίπεδο έτους και να το συγκρίνει με προκαθορισμένους στόχους. Επιπλέον, το ΠΙ θα πρέπει να διαθέτει διαδικασίες λεπτομερούς καταγραφής των συμβάντων μη διαθεσιμότητας (επηρεαζόμενα συστήματα, χρονική διάρκεια μη διαθεσιμότητας, αιτία προβλήματος, τρόπος και χρονική διάρκεια αντιμετώπισης, συχνότητα εμφάνισης, κόστος για το ΠΙ), άμεσης ενημέρωσης των αρμόδιων λειτουργικών μονάδων (Εσωτερικός Έλεγχος, Διαχείριση Κινδύνων) και της Διοίκησης.

11. επαρκείς διαδικασίες διαχείρισης αντιγράφων ασφαλείας (λεπτομερής αναφορά στο κεφάλαιο Γ4).

12. ειδικότερα, για τα συστήματα και τις υπηρεσίες Ηλεκτρονικής Τραπεζικής:

i. επαρκής πληροφόρηση στο διαδικτυακό τόπο (web site) του ΠΙ, έτσι ώστε να μπορούν οι εν δυνάμει πελάτες τους να έχουν μια επαρκή γνώση για την ταυτότητα του ΠΙ και την εποπτεύουσα αρχή που παρέχει την άδεια λειτουργίας, πριν πραγματοποιήσουν τις ηλεκτρονικές τους συναλλαγές. Επίσης, γνωστοποίηση του τρόπου με τον οποίο μπορούν να επικοινωνήσουν οι πελάτες με το σχετικό κέντρο υποστήριξης σε περίπτωση πάσης φύσεως προβλήματος, το ψηφιακό πιστοποιητικό του διαδικτυακού τόπου το οποίο θα πρέπει να έχει εκδοθεί από επίσημη αρχή πιστοποίησης, πληροφορίες για την ασφαλή χρήση των παρεχομένων υπηρεσιών κ.α.

ii. ενημέρωση των πελατών για την πολιτική εμπιστευτικότητας που εφαρμόζει το ΠΙ σε σχέση με τα προσωπικά τους δεδομένα. Η πληροφόρηση αυτή συνιστάται να παρέχεται και μέσα από το διαδικτυακό τόπο του ιδρύματος. Παροχή επίσης στους πελάτες του δικαιώματος να αρνηθούν την διάθεση - εκχώρηση σε τρίτους δεδομένων που τους αφορούν, για προώθηση προϊόντων ή άλλο λόγο. Τα δεδομένα των πελατών θα πρέπει να χρησιμοποιούνται μόνον για τους σκοπούς για τους οποίους οι πελάτες γνωρίζουν ότι τα διαθέτουν.

iii. σαφής σήμανση στο διαδικτυακό τόπο του ΠΙ των συνδέσεων (links) με διαδικτυακούς τόπους άλλων εταιρειών ή οργανισμών. Πρέπει να φαίνεται έκδηλα στον πελάτη ότι, όταν εγκαταλείπει το διαδικτυακό τόπο του ΠΙ, συνδέεται με μια εντελώς ξεχωριστή επιχειρηματική μονάδα ή άλλη νομική οντότητα.

iv. αυτοματοποιημένα συστήματα παρακολούθησης των συναλλαγών, τα οποία και θα βασίζουν την αποτελεσματι-

κή λειτουργία τους στη δημιουργία εκ μέρους του ΠΙ στατιστικών προτύπων κίνησης λογαριασμού για κάθε πελάτη. Τα συστήματα αυτά, με βάση τα διαμορφωμένα χαρακτηριστικά κίνησης των λογαριασμών των πελατών (profiles), θα πρέπει να εντοπίζουν και να καταγράφουν ασυνήθιστες συναλλακτικές συμπεριφορές και να παράγουν, σε πραγματικό χρόνο, προειδοποιητικά μηνύματα (alerts) για την διερεύνηση ενδεχόμενων περιπτώσεων απάτης.

v. αποτελεσματική αντιμετώπιση των κινδύνων νομιμοποίησης εσόδων από παράνομες δραστηριότητες (money laundering) και χρηματοδότησης τρομοκρατίας. Οι συγκεκριμένοι κίνδυνοι στην ηλεκτρονική τραπεζική είναι ιδιαίτερα αυξημένοι λόγω της ευκολίας χρήσης των υπηρεσιών από οπουδήποτε και οποιαδήποτε χρονική στιγμή, της απρόσωπης φύσης των συναλλαγών και της αυτόματης διεκπεραίωσης τους. Ως εκ τούτου, το ΠΙ θα πρέπει να μεριμνά για την εγκατάσταση αυτοματοποιημένων συστημάτων και εργαλείων διαχείρισης των συναλλαγών, τα οποία κατ' ελάχιστον θα θέτουν όρια σε συγκεκριμένες ομάδες ή κατηγορίες συναλλαγών, θα παρέχουν τη δυνατότητα καθυστέρησης εκτέλεσης της συναλλαγής μέχρι την εξακρίβωση συγκεκριμένων στοιχείων (filters & monitoring tools/systems) κ.α.

vi. δυνατότητα εύκολης προσπέλασης και επεξεργασίας στοιχείων παλαιότερων συναλλαγών, έτσι ώστε να γίνεται εφικτός ο εντοπισμός συναλλακτικών ιδιαιτεροτήτων και ανωμαλιών, για να διευκολύνεται η στοιχειοθέτηση αποδεικτικών στοιχείων και η επαρκής πληροφόρηση των εποπτικών αρχών, ειδικά στις περιπτώσεις απάτης και νομιμοποίησης εσόδων από παράνομες δραστηριότητες, παροχής επενδυτικών υπηρεσιών κ.λπ.

vii. εγχειρίδια σε ηλεκτρονική ή έντυπη μορφή, τα οποία θα ενημερώνουν τους πελάτες για τον τρόπο χρήσης των συστημάτων με έμφαση σε θέματα ασφάλειας. Επιπλέον, το ΠΙ θα πρέπει να εφοδιάζει τους χρήστες με πρακτικές ασφαλούς χρήσης των προσωπικών υπολογιστών μέσω των οποίων προσπελαύνονται ορισμένα συστήματα ηλεκτρονικής τραπεζικής και ηλεκτρονικών πληρωμών. Στις πρακτικές αυτές θα πρέπει να γίνεται αναφορά μεταξύ άλλων σε θέματα προστασίας από ιούς και άλλο κακόβουλο λογισμικό ασφαλούς αποθήκευσης και χρήσης προσωπικών κωδικών (ειδικά σε υπολογιστές κοινής χρήσης οι οποίοι γενικά θα πρέπει να αποφεύγονται για τέτοια χρήση) κ.α.

viii. επαρκείς διαδικασίες ασφάλειας με έμφαση στη πιστοποίηση των συναλλασσομένων μερών (ψηφιακό πιστοποιητικό διαδικτυακού τόπου ΠΙ, πιστοποίηση δύο επιπέδων για τον πελάτη, με χρήση ψηφιακών πιστοποιητικών, T.A.N. lists ή άλλης μεθόδου), τη μη αποποίηση των συναλλαγών, την κρυπτογράφηση της επικοινωνίας, την ασφάλεια των συναλλαγών (αποδεικτικά στοιχεία επιτυχούς ολοκλήρωσης, αποσύνδεση σε περίπτωση ανενεργού χρήστη, εντοπισμός ύποπτων συναλλαγών κ.λπ.), και τέλος τη λειτουργία των συστημάτων που υποστηρίζουν τις εν λόγω υπηρεσίες σε ειδικές περιοχές του δικτύου που παρέχουν υψηλή προστασία από κακόβουλες ενέργειες εσωτερικών ή εξωτερικών χρηστών.

Γ2. Φυσική Ασφάλεια

Ο όρος «Φυσική Ασφάλεια» αναφέρεται στα μέτρα που πρέπει να λαμβάνονται για την προστασία των συστημάτων και της υποδομής που τα υποστηρίζει, από κινδύνους που προέρχονται από το περιβάλλον. Ανάλυση κινδύνων είναι απαραίτητο να προηγείται της λήψης μέτρων, αφού οι απαιτήσεις φυσικής ασφάλειας δεν είναι δυνατόν να είναι οι ίδιες για όλες τις περιοχές και χώρους που στεγάζουν συστήματα, ούτε και η κρισιμότητα των συστημάτων είναι η ίδια μέσα σε μια συγκεκριμένη περιοχή ή χώρο.

Στα μέτρα φυσικής ασφάλειας πρέπει τουλάχιστον να περιλαμβάνονται:

1. μηχανισμοί ελέγχου φυσικής πρόσβασης (Physical Access Controls). Τέτοιοι μηχανισμοί πρέπει να περιορίζουν, να ελέγχουν και να καταγράφουν, αφ' ενός μεν την είσοδο και την έξοδο του προσωπικού και των επισκεπτών, αφ' ετέρου δε τη διακίνηση μηχανογραφικού εξοπλισμού και αποθηκευτικών μέσων. Μηχανισμοί ελέγχου φυσικής πρόσβασης θα πρέπει να υφίστανται, όχι μόνο σε χώρους που στεγάζουν μηχανογραφικό εξοπλισμό, αλλά και σε χώρους ή σημεία στα οποία υπάρχουν καλωδιώσεις που συνδέουν κρίσιμα συστήματα, υποστηρικτικές συσκευές (π.χ. μονάδες παροχής αδιάλειπτης τάσης, γεννήτριες), μαγνητικά μέσα στα οποία φυλάσσονται αρχεία, κ.λπ. Επιπλέον, η υλοποίηση τέτοιων μηχανισμών δεν θα πρέπει να περιορίζεται μόνο στους χώρους των μηχανογραφικών κέντρων, αλλά να επεκτείνεται και οπουδήποτε αλλού υπάρχει η σχετική ανάγκη (τοπικά συστήματα καταστημάτων και διευθύνσεων). Το είδος των μηχανισμών ελέγχου που υλοποιούνται θα πρέπει να καθορίζεται από την κρισιμότητα των συστημάτων που καλούνται να προστατεύσουν.

2. μηχανισμοί πρόληψης και αντιμετώπισης καταστροφών από φυσικά αίτια.

3. μηχανισμοί πρόληψης και αντιμετώπισης κακόβουλων ενεργειών (διάρρηξη / κλοπή, βανδαλισμός, τρομοκρατική ενέργεια, κ.λπ.). Οι συγκεκριμένοι κίνδυνοι, όπως και οι κίνδυνοι από φυσικά αίτια, εκτός του ότι μπορεί να προκαλέσουν ολοσχερή καταστροφή των συστημάτων και των δικτύων, είναι δυνατό να διακυβεύσουν τις ζωές του προσωπικού.

4. μηχανισμοί πρόληψης και αντιμετώπισης προβλημάτων από διακοπή λειτουργίας και παροχής υπηρεσιών ή βλάβη υποστηρικτικών συσκευών. Τα συστήματα είναι απαραίτητο να λειτουργούν σε ένα αποτελεσματικά υποστηριζόμενο τεχνικά περιβάλλον.

5. η αποτελεσματική διαχείριση της τηλεπικοινωνιακής και δικτυακής καλωδίωσης για την αντιμετώπιση θέματα φθοράς, παρεμβολών και έλλειψης κατάλληλης σήμανσης.

6. μηχανισμοί ασφάλειας φορητών συστημάτων. Η χρήση των φορητών υπολογιστών και οποιωνδήποτε άλλων φορητών συστημάτων θα πρέπει να λαμβάνεται σοβαρά υπόψη στην ανάλυση κινδύνων. Φορητοί υπολογιστές που αποθηκεύουν ευαίσθητα εταιρικά δεδομένα θα πρέπει, αφ' ενός μεν να φυλάσσονται σε ασφαλή σημεία όταν δεν είναι σε χρήση, αφ' ετέρου δε να αποθηκεύουν τα ευαίσθητα δεδομένα σε κρυπτογραφημένη μορφή.

7. η ασφαλής μεταφορά και αποθήκευση των ευαίσθητων εγγράφων και μαγνητικών μέσων. Στην πρώτη κατηγορία ανήκουν οι διαβαθμισμένες αναφορές, οι εφεδρικοί κωδικοί εισόδου των διαχειριστών συστημάτων, τα συνθηματικά των πελατών μέχρι να τους αποσταλούν, η τεκμηρίωση των συστημάτων και εφαρμογών, τα Σχέδια Συνέχειας Εργασιών και Ανάκαμψης από Καταστροφή, κα. Στην δεύτερη ανήκουν τα εφεδρικά αντίγραφα αρχείων, το πλαστικό υλικό των καρτών συναλλαγών κ.λπ.

8. η επιλογή και κατάλληλη διαμόρφωση των χώρων με σκοπό την ελαχιστοποίηση των προαναφερθέντων κινδύ-

νων, σε σχέση πάντοτε με τη χρήση για την οποία προορίζονται και την κρισιμότητα των συστημάτων που στεγάζουν.

Γ3. Λογική ασφάλεια

Ο όρος «λογική ασφάλεια» αναφέρεται στο σύνολο των μέτρων που λαμβάνονται για τον περιορισμό της πρόσβασης στους πόρους των συστημάτων (system resources). Ως πόροι των συστημάτων θεωρούνται ο μηχανογραφικός εξοπλισμός, τα δίκτυα, το λογισμικό και τα δεδομένα. Τα μέτρα που υλοποιούν την λογική ασφάλεια καθορίζουν όχι μόνον το «ποιος» ή «τι» (π.χ. πρόγραμμα) θα έχει πρόσβαση σε συγκεκριμένους πόρους του συστήματος, αλλά και το είδος της πρόσβασης που επιτρέπεται να έχει. Τα μέτρα αυτά μπορεί να είναι ενσωματωμένα στα λειτουργικά συστήματα, να υλοποιούνται σε προγράμματα εφαρμογών, σε συστήματα διαχείρισης βάσεων δεδομένων, σε συστήματα επικοινωνιών ή ακόμη να υλοποιούνται μέσω πρόσθετων αυτόνομων πακέτων ασφάλειας.

Για την διατήρηση ενός αποδεκτού επιπέδου λογικής ασφαλείας, κρίνεται σκόπιμο:

(α) για την ασφάλεια των προσβάσεων στα συστήματα

1. να έχουν όλοι οι χρήστες ένα μοναδικό ατομικό λογαριασμό πρόσβασης σε κάθε σύστημα και μόνο για τους πόρους εκείνους που δικαιούνται πρόσβαση, ώστε κάθε ενέργεια να χρεώνεται μονοσήμαντα. Ως εκ τούτου, κοινοί - ομαδικοί λογαριασμοί πρόσβασης δεν θα πρέπει να χρησιμοποιούνται, και όπου αυτό δεν είναι εφικτό, θα πρέπει οι ενέργειες των κατόχων των λογαριασμών αυτών να καταγράφονται και να ελέγχονται σχολαστικά.

2. να υπάρχουν καταγεγραμμένες και εγκεκριμένες διαδικασίες για τη διαχείριση των λογαριασμών πρόσβασης, τον καθορισμό και την αναθεώρηση των δικαιωμάτων που παρέχονται στον κάθε λογαριασμό για όλα τα στάδια της εργασιακής πορείας του ιδιοκτήτη του λογαριασμού (πρόσληψη, μετακίνηση, αλλαγή αντικειμένου εργασίας, αποχώρηση κ.λπ.). Να υπάρχει διαχωρισμός αρμοδιοτήτων στην έγκριση, υλοποίηση και έλεγχο των προσβάσεων.

3. να καταγράφονται και να ελέγχονται συστηματικά οι ενέργειες που γίνονται με χρήση λογαριασμών πρόσβασης με προνομιακά δικαιώματα, όπως λογαριασμών διαχειριστών συστημάτων και γενικά χρηστών με αυξημένα δικαιώματα.

4. οι λογαριασμοί πρόσβασης να απενεργοποιούνται άμεσα μόλις παύουν να είναι απαραίτητοι ή σε περίπτωση σημαντικής παραβίασης των κανόνων ασφάλειας.

5. να υπάρχει συγκεκριμένη διαδικασία που να προβλέπει τη δημιουργία προσωρινών λογαριασμών πρόσβασης, με καθορισμένο επίπεδο εξουσιοδοτήσεων, για συγκεκριμένες εργασίες ή για περιπτώσεις ανάγκης. Η χρήση των λογαριασμών αυτών θα πρέπει να ελέγχεται σχολαστικά, και μόλις εκλείψει η ανάγκη για την οποία δημιουργήθηκαν θα πρέπει να απενεργοποιούνται.

6. να πιστοποιείται ο ιδιοκτήτης ενός λογαριασμού πρόσβασης, κατά τη διαδικασία εισόδου του στο σύστημα μέσω μιας διαδικασίας υψηλής ασφάλειας (όπως π.χ. κωδικός εισόδου, χρήση «έξυπνης» κάρτας, ψηφιακού πιστοποιητικού κλπ)

7. να αλλάζονται άμεσα οι κωδικοί πρόσβασης που έχουν τεθεί από τις κατασκευάστριες εταιρείες σε κάθε νέο τεχνολογικό εξοπλισμό μετά την παραλαβή του.

8. οι κωδικοί πρόσβασης:

• να δημιουργούνται και να γίνεται η διαχείρισή τους βάσει προτύπων και διαδικασιών

• να είναι δύσκολα προβλέψιμοι

• να διατηρούνται μυστικοί με ευθύνη των κατόχων τους

• να αλλάζουν σε τακτική βάση και οπωσδήποτε την πρώτη φορά εισόδου του κατόχου τους στο σύστημα. Η αλλαγή των κωδικών να επιβάλλεται από το σύστημα, και να κρατείται ιστορικό αλλαγών για την αποφυγή επανάληψης των ίδιων κωδικών, εφόσον αυτό είναι εφικτό

9. οι εφεδρικοί κωδικοί των διαχειριστών συστημάτων ή λογαριασμών ειδικών προνομίων θα πρέπει να βρίσκονται αποθηκευμένοι σε ασφαλές σημείο, ώστε να μπορούν να χρησιμοποιηθούν βάσει ειδικής διαδικασίας σε περίπτωση έκτακτης ανάγκης.

10. όπου κρίνεται αναγκαίο, οι κωδικοί πρόσβασης λογαριασμών ειδικών προνομίων θα πρέπει να μη φυλάσσονται ενιαίοι, αλλά σε τμήματα με ευθύνη διαφορετικών ατόμων.

11. να χρησιμοποιείται - όπου είναι εφικτό - ειδικό λογισμικό διαχείρισης και ελέγχου των προσβάσεων.

(β) για την προστασία των δεδομένων

1. να υπάρχουν επαρκείς ενσωματωμένοι μηχανισμοί ελέγχου (controls) των δεδομένων στα διάφορα συστήματα, και ειδικότερα, στην προετοιμασία, εισαγωγή, και επεξεργασία τους.

2. να υπάρχει καταγεγραμμένη και εγκεκριμένη διαβάθμιση των δεδομένων σύμφωνα με το βαθμό ευαισθησίας τους και να προβλέπονται επιπλέον διαδικασίες ασφάλειας των ευαίσθητων δεδομένων μέσω τεχνικών κρυπτογράφησης ή άλλων μεθόδων προστασίας.

3. για την κρυπτογράφηση:

• να καθορίζεται σαφώς το πότε και σε ποιο επίπεδο γίνεται κρυπτογράφηση

• να χρησιμοποιείται υψηλής ασφάλειας κλειδί κρυπτογράφησης σε όλο το λογισμικό

• να αναπτύσσεται στρατηγική υποδομής Δημόσιου Κλειδιού P.K.I. (public key infrastructure) για τη διαχείριση των ψηφιακών πιστοποιητικών, κυρίως για την επικοινωνία του ΠΙ με τους πελάτες του για παροχή υπηρεσιών ηλεκτρονικής τραπεζικής

• να επιδιώκεται η συμμόρφωση με τους εθνικούς και διεθνείς κανονισμούς και πρακτικές κρυπτογράφησης

4. να γίνονται οι απαραίτητες ενέργειες για τη συμμόρφωση με τη σχετική νομοθεσία και τους κανονισμούς Προστασίας Δεδομένων.

5. να υπάρχει πολιτική σχετικά με την ενημέρωση των πελατών στην περίπτωση διαρροής εμπιστευτικών προσωπικών τους δεδομένων λόγω παραβίασης της ασφάλειας των συστημάτων.

6. για τις βάσεις δεδομένων:

• να υπάρχει ολοκληρωμένη και ακριβής τεκμηρίωση της βάσης που να περιλαμβάνει τουλάχιστον τον λογικό σχεδιασμό, τον φυσικό σχεδιασμό και το λεξικό δεδομένων

• να γίνεται αναδιοργάνωση της βάσης σε τακτά χρονικά διαστήματα

• να εξασφαλίζεται η καταχώρηση μόνο ολοκληρωμένων συναλλαγών (commit / rollback)

(γ) Για την προστασία των συστημάτων

1. να υπάρχει εγκαταστημένο κατ' ελάχιστο στα κρίσιμα συστήματα, και όπου αλλού είναι αναγκαίο ειδικό λογισμικό προστασίας από ιούς ή άλλο «κακόβουλο» λογισμικό. Το λογισμικό προστασίας θα πρέπει να ενημερώνεται σε συνεχή βάση και να είναι εγκαταστημένο με τέτοιο τρό-

πο ώστε να ενεργοποιείται αυτόματα και να μην μπορεί να απενεργοποιηθεί από τους χρήστες των συστημάτων, παρά μόνο από τον αρμόδιο διαχειριστή.

2. να παρέχεται αποτελεσματική προστασία σε ευαίσθητους πόρους των συστημάτων, όπως τα αρχεία συστήματος και εφαρμογών.

3. να συντηρείται αρχείο με το εγκεκριμένο από το ΠΙ λογισμικό

4. να απεγκαθίσταται ή να απενεργοποιείται σε κάθε σύστημα, κάθε λογισμικό ή λειτουργία που δεν κρίνεται απαραίτητη.

5. να ενεργοποιούνται τουλάχιστον οι βασικές λειτουργίες ελέγχου και καταγραφής (auditing & logging functions) σε κάθε σύστημα και να παραμετροποιούνται κατάλληλα σε συνεργασία με τον εσωτερικό έλεγχο.

6. να εξασφαλίζεται όπου αυτό είναι αναγκαίο, κατόπιν σχετικής εγκριτικής διαδικασίας, η συνεχής ενημέρωση των συστημάτων με τις τελευταίες εκδόσεις λογισμικού και ενημερώσεων σε θέματα ασφάλειας, ώστε να ελαχιστοποιούνται οι αδυναμίες και τα τρωτά τους σημεία.

7. να υπάρχουν καταγεγραμμένες διαδικασίες αποκατάστασης της ασφαλούς λειτουργίας ενός συστήματος σε περίπτωση που παραβιαστεί η ασφάλεια του.

8. να προστατεύεται, όσο αυτό είναι εφικτό, το ηλεκτρονικό ταχυδρομείο από πιθανούς κινδύνους αναξιόπιστης γνησιότητας του αποστολέα, υποκλοπής ή και παραποίησης του περιεχομένου, επικίνδυνων προσαρτημάτων, ανεπιθύμητων μηνυμάτων κ.λπ.

9. να υπάρχουν περιορισμοί στις ενέργειες των χρηστών του Διαδικτύου (π.χ. στις προσβάσεις σε συγκεκριμένους διαδικτυακούς τόπους, στη διακίνηση αρχείων κ.λπ.).

10. να γίνεται συνεχής εκπαίδευση και ενημέρωση των χρηστών σε θέματα ασφαλούς λειτουργίας των συστημάτων.

11. να προστατεύονται αποτελεσματικά τα κρίσιμα συστήματα από κακόβουλες ενέργειες εξωτερικών ή εσωτερικών χρηστών. Προς αυτή την κατεύθυνση οφείλουν να υλοποιούνται διάφορες τεχνικές, όπως:

- η χρήση ειδικών συστημάτων (firewalls, filtering routers κλπ), τα οποία, ως σημεία ελέγχου των προσβάσεων, θα ρυθμίζουν και θα ελέγχουν την επικοινωνία από και προς περιοχές του δικτύου οι οποίες είναι συνήθως εκτεθειμένες σε αυξημένους κινδύνους
- η δημιουργία στο δίκτυο ειδικών περιοχών (Demilitarized Zones - DMZ), ανάμεσα σε σημεία ελέγχου προσβάσεων, οι οποίες να λειτουργούν σαν απομονωμένο δίκτυο για τα προσβάσιμα από εσωτερικούς ή εξωτερικούς χρήστες συστήματα του ΠΙ, προστατεύοντας έτσι αποτελεσματικά το υπόλοιπο δίκτυο από κακόβουλες ενέργειες

(δ) για την ασφάλεια της δικτυακής υποδομής και των επικοινωνιών

1. να είναι σαφώς καθορισμένες, καταγεγραμμένες και ελεγχόμενες οι δίοδοι επικοινωνίας (gateways) με εξωτερικά δίκτυα.

2. να εκτιμάται η δυνατότητα κατάτμησης (segmentation) του δικτύου σε ελεγχόμενα επί μέρους υποδίκτυα για τον καλύτερο έλεγχο των προσβάσεων.

3. να μην παραμένουν ανοιχτές λογικές θύρες επικοινωνίας (ports) σε κάθε συσκευή του δικτύου, επιπλέον όσων έχουν καθοριστεί σαφώς ως αναγκαίες για τις υπηρεσίες που υποστηρίζουν και αφού έχει συνεκτιμηθεί ο συνεπαγόμενος κίνδυνος από τη λειτουργία τους.

4. να περιορίζεται και να ελέγχεται επαρκώς η πρόσβαση στις ειδικές λειτουργίες διαχείρισης και ελέγχου του δικτύου.

5. να υπάρχει αποτελεσματική διαχείριση των παραμετροποιήσεων των συσκευών του δικτύου.

6. να υπάρχει η δυνατότητα εντοπισμού από το διαχειριστή του δικτύου λειτουργίας μη εξουσιοδοτημένων συσκευών.

7. να περιορίζονται στα απολύτως απαραίτητα τα σημεία πρόσβασης στο δίκτυο τα οποία βρίσκονται σε χώρους μη ελεγχόμενης φυσικής πρόσβασης, και εφόσον δε χρησιμοποιούνται να είναι ανενεργά.

8. να περιορίζεται και να ελέγχεται συστηματικά η δυνατότητα ασύρματης σύνδεσης χρηστών στο δίκτυο, ώστε να αποτρέπεται η παρείσφρηση μη εξουσιοδοτημένων χρηστών σε αυτό.

9. να μην παρέχεται η δυνατότητα απομεμακρυσμένης πρόσβασης στο δίκτυο, και όπου κρίνεται αναγκαία τέτοια πρόσβαση, να καταγράφεται και να ελέγχεται συστηματικά. Ειδικότερα, σε περίπτωση πρόσβασης στο δίκτυο χρηστών μέσω τηλεφωνικής σύνδεσης (dial up), αυτή να πραγματοποιείται κατόπιν διαδικασίας επιστροφής κλήσης (call back) ή άλλης κατάλληλης μεθόδου επαλήθευσης του καλούντος.

10. να χρησιμοποιούνται τα κατάλληλα πρωτόκολλα επικοινωνίας ανάλογα με το είδος των δεδομένων που μεταδίδοντας αντιμετωπίζοντας αποτελεσματικά θέματα διαχείρισης και ασφάλειας τους.

11. να εξασφαλίζεται η εμπιστευτικότητα και η ακεραιότητα των δεδομένων που μεταδίδονται μέσω του δικτύου καθ' όλη τη διαδρομή τους σε αυτό.

12. να γίνεται χρήση ειδικών εργαλείων λογισμικού για τον εντοπισμό κενών ασφαλείας ή σημείων μειωμένης ασφάλειας στο δίκτυο (vulnerability tests).

13. να υπάρχουν διαδικασίες και συστήματα παρακολούθησης, αποτροπής και αντιμετώπισης προσπαθειών παρείσφρησης στο δίκτυο ή γενικότερα προσπαθειών παραβίασης της ασφάλειας του δικτύου (intrusion detection/prevention systems).

14. να διενεργούνται σε τακτική βάση, από ειδικευμένες εταιρίες, δοκιμαστικές απόπειρες παραβίασης της ασφάλειας του δικτύου (penetration tests), βάσει καθορισμένων σεναρίων, με στόχο την αξιολόγηση της επάρκειας της ασφάλειας του δικτύου.

Γ4. Σχέδια Συνέχειας Εργασιών & Ανάκαμψης από Καταστροφή

Το ΠΙ πρέπει να διαθέτει εγκεκριμένα από τη Διοίκηση Σχέδια Συνέχειας Εργασιών (ΣΣΕ) για τα Πληροφοριακά Συστήματα, ενταγμένα στα γενικότερα εταιρικά ΣΣΕ, έτσι ώστε να εξασφαλίζεται η συνέχεια των κρισιμότερων λειτουργιών τους. Επιπλέον, το ΠΙ πρέπει να διαθέτει αποτελεσματικά Σχέδια Ανάκαμψης από Καταστροφή (ΣΑΚ) που θα εφαρμόζονται στις περιπτώσεις καταστροφικών συμβάντων που μπορεί να προκαλέσουν παρατεταμένη διακοπή της λειτουργίας ενός κρίσιμου συστήματος, ή ακόμη και ολόκληρου του μηχανογραφικού κέντρου.

Της δημιουργίας ΣΣΕ και ΣΑΚ θα πρέπει να προηγούνται διαδικασίες ανάλυσης επιχειρηματικών επιπτώσεων (business impact analysis) και ανάλυσης κινδύνων (risk assessment). Βάσει αυτών:

- θα προσδιορίζονται όλες οι κρίσιμες λειτουργίες καθώς και τα συστήματα-πόροι που χρησιμοποιούν

• θα προσδιορίζονται όλοι οι κίνδυνοι που απειλούν τις κρίσιμες λειτουργίες και θα κατατάσσονται σύμφωνα με την πιθανότητα εμφάνισης τους και τις πιθανές επιπτώσεις τους στα συστήματα και τις λειτουργίες

• θα σταθμίζεται το λειτουργικό κόστος από ενδεχόμενη διακοπή των κρίσιμων λειτουργιών και το κόστος ενεργοποίησης του ΣΣΕ & ΣΑΚ για να προσδιορίζονται οι συνθήκες που θα θέτουν σε εφαρμογή το αντίστοιχο σχέδιο

• θα προσδιορίζεται ο χρόνος ανάκαμψης των κρισίμων λειτουργιών - συστημάτων (recovery time) αλλά και το σημείο ανάκαμψης (recovery point), δηλαδή σε πόσο χρόνο και σε ποια εικόνα χρονικά θα επανέλθουν τα συστήματα μετά την ανάκαμψη

Πρώτο επίπεδο εξασφάλισης συνέχειας εργασιών θεωρείται η ύπαρξη σχεδίου λήψης και διαχείρισης αντιγράφων ασφαλείας του λογισμικού, των παραμέτρων λειτουργίας και των δεδομένων, καθώς και η ύπαρξη του αναγκαίου εφεδρικού εξοπλισμού, συσκευών παροχής αδιάλειπτης τάσης, ηλεκτρογεννητριών κ.λπ., στους χώρους λειτουργίας των συστημάτων.

Με στόχο την εξασφάλιση της γρήγορης και επιτυχούς ανάκτησης των δεδομένων και του λογισμικού, θα πρέπει για τα αντίγραφα ασφαλείας να υφίστανται συγκεκριμένες διαδικασίες:

• δημιουργίας με συχνότητα που υπαγορεύεται από τη κρισιμότητα των πληροφοριών

• ασφαλούς φύλαξης στο χώρο των συστημάτων

• ασφαλούς μεταφοράς και φύλαξης σε απομεμακρυσμένο χώρο των επιπλέον αντιγράφων

• δοκιμών για τη διασφάλιση της ακεραιότητας των δεδομένων

• αρχειοθέτησης με αναγραφή στα μέσα αποθήκευσης του περιεχομένου και του χρόνου αποθήκευσης των δεδομένων

• ανακύκλωσης των μαγνητικών μέσων.

Σε δεύτερο επίπεδο, ένα ολοκληρωμένο και αποτελεσματικό ΣΣΕ δι ΣΑΚ για τα ΠΣ, συνιστάται:

1. να είναι γραμμένο σε απλή και κατανοητή γλώσσα και να κοινοποιείται επίσημα σε όλο το προσωπικό. Τυχόν διαβαθμισμένες πληροφορίες του σχεδίου (όπως π.χ. κωδικοί, κλείδες ασφαλείας κ.λπ.), θα πρέπει να γνωστοποιούνται μόνο σε εξουσιοδοτημένο προσωπικό.

2. αντίγραφο του να φυλάσσεται σε κατάλληλο χώρο σε ασφαλή απόσταση από το μηχανογραφικό κέντρο.

Ένα τέτοιο σχέδιο θα πρέπει να περιλαμβάνει:

3. κατάταξη των συστημάτων βάση λειτουργικής ανάγκης. Στην κατάταξη αυτή θα πρέπει, μεταξύ άλλων, να αναφέρεται ο χρόνος που απαιτείται για την ανάκτηση (recovery time) του κάθε συστήματος καθώς και η ελάχιστη εκτιμώμενη απόδοση του μετά την ανάκτηση.

4. τη σαφή ιεραρχική δομή των στελεχών που συμμετέχουν στην εφαρμογή του, τις αρμοδιότητές τους, καθώς και τους υπεύθυνους λήψης αποφάσεων σε κάθε ομάδα έκτακτης ανάγκης.

5. τις διαδικασίες εκτίμησης του εύρους της καταστροφής, με βάση τις οποίες προσδιορίζονται επακριβώς τα τμήματα του σχεδίου τα οποία θα πρέπει να ενεργοποιηθούν.

6. τις διαδικασίες ενεργοποίησης του σχεδίου, ειδοποίησης των στελεχών και κινητοποίησης των ομάδων έκτακτης ανάγκης.

7. τις ενέργειες που θα εκτελούνται σε συγκεκριμένες επείγουσες καταστάσεις, οι οποίες μεταξύ των άλλων θα πρέπει να διασφαλίζουν το προσωπικό σε περίπτωση κινδύνου / καταστροφής (π.χ. φωτιά, σεισμός κ.λπ.).

8. τους εναλλακτικούς χώρους εργασίας των χρηστών, τον εξοπλισμό που θα χρησιμοποιηθεί, καθώς και τις απαιτούμενες προδιαγραφές τους.

9. τις διαδικασίες προετοιμασίας και ενεργοποίησης του εναλλακτικού μηχανογραφικού κέντρου.

10. τα συστήματα του εναλλακτικού κέντρου, την υποδομή τους καθώς και την τοπολογία δικτύου.

11. λίστα προμηθευτών με τους οποίους υπάρχουν συμβάσεις, οι υπηρεσίες που αυτοί προσφέρουν και οι αναμενόμενοι χρόνοι απόκρισης τους σε περίπτωση έκτακτης ανάγκης.

12. τις διαδικασίες που εξασφαλίζουν ότι τα σχέδια συντηρούνται, προσαρμόζονται και ενημερώνονται σε κάθε αλλαγή στις διαδικασίες λειτουργίας του ΠΙ.

13. τις διαδικασίες εκπαίδευσης του προσωπικού σύμφωνα με τις αρμοδιότητες που αναλαμβάνουν κατά την υλοποίηση του Σχεδίου.

14. τις διαδικασίες εκτέλεσης δοκιμών, σύμφωνα με τις οποίες:

• θα προσδιορίζεται η συχνότητά τους (κατ' ελάχιστο μία φορά το χρόνο)

• θα υπάρχουν σαφείς στόχοι εκ των προτέρων, είτε για την εξέταση συγκεκριμένων υποσυστημάτων, είτε για την εξέταση του συστήματος στο σύνολο του. Η εκτέλεση δοκιμών της τελευταίας κατηγορίας συνιστάται να περιλαμβάνει την πλήρη κάλυψη όλων των κρίσιμων λειτουργιών όπως αναγράφονται στο σχέδιο και να κάνει αποκλειστική χρήση του εναλλακτικού χώρου, του εξοπλισμού και των εφεδρικών αντιγράφων

• θα διεξάγονται υπό συνθήκες που θα προσομοιώνουν περιπτώσεις έκτακτης ανάγκης

• θα εξασφαλίζεται η συμμετοχή του εσωτερικού ελέγχου

• θα συντάσσεται έκθεση των αποτελεσμάτων μετά την ολοκλήρωση των δοκιμών

• θα γίνονται οι απαραίτητες διορθώσεις στα σχέδια για όλα τα προβλήματα που διαπιστώνονται

• θα λαμβάνει γνώση των αποτελεσμάτων η Διοίκηση και η Επιτροπή Ελέγχου Τέλος, θα πρέπει:

15. να εξασφαλίζει την αποτελεσματική λειτουργία εναλλακτικού μηχανογραφικού κέντρου, το οποίο θα πρέπει να βρίσκεται σε κατάλληλη απόσταση, ώστε να μην επηρεάζεται από τους ίδιους κινδύνους που μπορεί να πλήξουν το κύριο μηχανογραφικό κέντρο. Το εναλλακτικό κέντρο θα πρέπει να διαθέτει κατάλληλο (εφεδρικό) εξοπλισμό που να παρέχει όλες τις κρίσιμες υπηρεσίες στους χρόνους που έχουν προκαθοριστεί, καθώς και τα εγχειρίδια των διαδικασιών και χρήσης των συστημάτων. Επιπλέον, θα πρέπει να επιτρέπει την απρόσκοπτη χρήση των εναλλακτικών μέσων μέχρι τη στιγμή της επαναφοράς των λειτουργιών στο κύριο μηχανογραφικό κέντρο.

16. να διασφαλίζει τη φυσική ασφάλεια του εναλλακτικού κέντρου, καθώς και ένα βασικό επίπεδο λογικής ασφάλειας κατά την εφαρμογή του σχεδίου.

17. να φροντίζει για την ασφαλιστική κάλυψη του ΠΙ απέναντι σε κινδύνους που είναι δυνατόν να προκαλέσουν διακοπή της λειτουργίας των Πληροφοριακών Συστημάτων.

18. σε περίπτωση που οι χώροι λειτουργίας του εναλλακτικού κέντρου, ο εξοπλισμός ή οι υπηρεσίες παρέχονται από τρίτους:

• να προνοεί, μέσω κατάλληλων συμβάσεων, για την αποτελεσματική συνέχεια των εργασιών σε περίπτωση καταστροφής που θα πλήξει ταυτόχρονα πολλούς οργανισμούς οι οποίοι εξυπηρετούνται από τον ίδιο πάροχο

• να φροντίζει για την ενημέρωση του παρόχου για τυχόν αλλαγές στα συστήματα που πιθανό να απαιτήσουν αντίστοιχες προσαρμογές - ενημερώσεις στα ΣΑΚ

Δ. ΕΛΕΓΧΟΣ ΣΥΣΤΗΜΑΤΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ

Μια αποτελεσματική ελεγκτική λειτουργία για τα Πληροφοριακά Συστήματα θα πρέπει να εστιάζεται στους κινδύνους που απορρέουν από την ανάπτυξη, ενσωμάτωση και λειτουργία τους, να εξετάζει την επάρκεια των ελεγκτικών μηχανισμών (controls) και διαδικασιών, και να προτείνει, όπου χρειάζεται, τις κατάλληλες τροποποιήσεις. Επιπλέον, θα πρέπει να αξιολογεί το βαθμό συμμόρφωσης με την επιχειρησιακή στρατηγική και τις καταγεγραμμένες επιχειρησιακές πολιτικές, τα πρότυπα και τις διαδικασίες, και να παρακολουθεί το βαθμό συμμόρφωσης με τις διαπιστώσεις των πορισμάτων των ελέγχων. Τέλος θα πρέπει να υπάρχει ολοκληρωμένη εικόνα για τη λειτουργία των Πληροφοριακών Συστημάτων ώστε να δίνεται η δυνατότητα επαρκούς ενημέρωσης σε τακτική βάση της Επιτροπής Ελέγχου.

Για τους λόγους αυτούς, η υπηρεσιακή μονάδα του Εσωτερικού Ελέγχου θα πρέπει:

1. να διαθέτει την τεχνογνωσία, την ποιοτική και ποσοτική επάρκεια προσωπικού, μέσων και διαδικασιών για τη διενέργεια εξειδικευμένων ελέγχων στα Πληροφοριακά Συστήματα. Η τεχνογνωσία και η εκπαίδευση του προσωπικού θα πρέπει να είναι τέτοιες ώστε να καλύπτονται ελεγκτικά οι τρέχουσες και οι μελλοντικές μηχανογραφικές λειτουργίες του ΠΙ.

2. να καταρτίζει και να υλοποιεί ελεγκτικό πρόγραμμα το οποίο θα βασίζεται σε ανάλυση κινδύνων που έχει διενεργηθεί στα Πληροφοριακά Συστήματα αλλά και σε ευρήματα προγενέστερων ελέγχων.

3. να ακολουθεί καταγεγραμμένες διαδικασίες σχεδιασμού, οργάνωσης και διενέργειας των ελέγχων, συγγραφής των πορισμάτων καθώς και διαδικασίες επανελέγχου (follow-up). Οι διαδικασίες αυτές, τα κάθε είδους ερωτηματολόγια που χρησιμοποιούνται στους εξειδικευμένους ελέγχους, καθώς και η χρησιμοποιούμενη μεθοδολογία ανάλυσης μηχανογραφικών κινδύνων, θα πρέπει να αποτελούν την επίσημη τεκμηρίωση της λειτουργίας του ελέγχου των Πληροφοριακών Συστημάτων.

4. να παρακολουθεί τα θέματα που αφορούν στα Πληροφοριακά Συστήματα του ΠΙ, ώστε να διαμορφώνει εικόνα για τους κινδύνους που υπάρχουν ή ενδέχεται να ανακύψουν. Για τη διαμόρφωση όσο το δυνατόν πληρέστερης εικόνας, συνιστάται η παρακολούθηση της λειτουργίας των Πληροφοριακών Συστημάτων μέσω ειδικών προσβάσεων, η συμμετοχή στις διάφορες επιτροπές έργων και η ύπαρξη διαδικασιών και μηχανισμών άμεσης ενημέρωσης του εσωτερικού ελέγχου στις περιπτώσεις εμφάνισης σημαντικών προβλημάτων και εκτάκτων περιστατικών.

5. να κάνει χρήση - ανάλογα με την περίπτωση - ειδικού ελεγκτικού λογισμικού για τον αποτελεσματικότερο έλεγχο της ασφάλειας των συστημάτων και της ακεραιότητας των δεδομένων τους.

6. να συμμετέχει στη φάση σχεδιασμού των συστημάτων για τη διαμόρφωση των κατάλληλων δικλείδων ασφαλείας, των ελεγκτικών αρχείων καταγραφής και αναφορών που παράγονται για τη διευκόλυνση του ελέγχου, καθώς και στη φάση των δοκιμών.

7. να ελέγχει και να αξιολογεί τις διαδικασίες παραγωγής των στοιχείων που υποβάλλονται στη Διοίκηση του ΠΙ και τις Εποπτικές Αρχές, ώστε να διασφαλίζεται η πληρότητα και ακρίβεια τους.

8. να μεριμνά για την άμεση και πλήρη ενημέρωση, στις περιπτώσεις σοβαρών προβλημάτων και έκτακτων περιστατικών στα Πληροφοριακά Συστήματα (περιπτώσεις απάτης, παραβίασης της ασφάλειας σημαντικών συστημάτων, μη διαθεσιμότητας κρισίμων συστημάτων, ενεργοποίησης Σχεδίων Ανάκαμψης από Καταστροφή), της αρμόδιας υπηρεσιακής μονάδας της Διεύθυνσης Εποπτείας Πιστωτικού Συστήματος της Τράπεζας της Ελλάδος, σύμφωνα με τις ισχύουσες διατάξεις.

9. να ελέγχει και να αξιολογεί την επάρκεια και συμμόρφωση με τις διαδικασίες που διέπουν τις φάσεις συνεργασίας του ΠΙ (επιλογή συνεργάτη, σύναψη και τήρηση συμβολαίου, ποιότητα παρεχόμενων υπηρεσιών) με προμηθευτές και παρόχους μηχανογραφικών υπηρεσιών βάσει των προαναφερθέντων στην ενότητα Α3.

10. να επιβλέπει το ελεγκτικό έργο στα πληροφορικής σε επίπεδο ομίλου. Για το σκοπό αυτό οφείλει να διατηρεί διαύλους επικοινωνίας με στόχο την αποτελεσματική συνεργασία με τις διοικήσεις και τον εσωτερικό έλεγχο των θυγατρικών και του δικτύου καταστημάτων εξωτερικού. Να αξιολογεί την επάρκεια του ελεγκτικού έργου μέσω περιοδικών αναφορών ή και συμμετοχής του στις επιτροπές ελέγχου των θυγατρικών, ειδικά σε αυτές που το μέγεθος και η πολυπλοκότητα των συστημάτων το καθιστούν αναγκαίο. Να αξιολογεί την επάρκεια των διενεργούμενων εξειδικευμένων ελέγχων από εσωτερικούς και εξωτερικούς ελεγκτές. Να προβαίνει σε γενικούς ή ειδικούς ελέγχους ανά περίπτωση, για την κάλυψη των ελεγκτικών αναγκών που είτε δεν καλύπτονται επαρκώς από τον εσωτερικό έλεγχο των εν λόγω μονάδων, είτε κρίνονται απαραίτητοι από τη σχετική ανάλυση κινδύνων.

11. να μελετά, αξιολογεί και εφαρμόζει, όπου κρίνει πρόσφορο, τα διεθνή πρότυπα και μεθοδολογίες ελέγχου Πληροφοριακών Συστημάτων.

Σε ό,τι αφορά στους ελέγχους που ανατίθενται σε εξωτερικούς ελεγκτές, το ΠΙ θα πρέπει:

να διαθέτει πολιτική για το εύρος και το ρόλο του εξωτερικού ελέγχου στα Πληροφοριακά Συστήματα, καθώς και διαδικασίες αξιολόγησης των προσφερομένων υπηρεσιών. Η πολιτική θα πρέπει να τεκμηριώνει τις περιπτώσεις που ο εξωτερικός έλεγχος δρα, είτε παράλληλα με τον εσωτερικό προσφέροντας μία επιπλέον εξειδικευμένη άποψη, είτε συμπληρωματικά προκειμένου να καλύψει εξειδικευμένες ελεγκτικές απαιτήσεις όπου δεν υπάρχει η δυνατότητα να καλυφθούν εσωτερικά, ή και με τους δύο τρόπους.

ΑΠΟ ΤΟ ΕΘΝΙΚΟ ΤΥΠΟΓΡΑΦΕΙΟ